International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN (Online): 2347-5552, Volume-14, Issue-3, May 2026
DOI: https://doi.org/10.55524/ijircst.2026.14.3.9
Article ID IRPC-1424, Pages 75-88
www.ijircst.org

Secure Academic Certificate Verification Using Blockchain and SHA-256 Cryptographic Hashing

Krishna Kr Mohan[1], and Dr. Shrikrishna S Balwante[2]

[1] M.Tech Scholar, Department of Computer Science & Engineering,
G H Raisoni International Skill Tech University, Pune, India
[2] Associate Professor & Head, Department of Computer Science & Engineering,
G H Raisoni International SkillTech University, Pune, India

*Correspondence should be addressed to Krishna Kr Mohan; krishnamohan.kumar@gmail.com

Received: 27 April 2026; Revised: 12 May 2026; Accepted: 26 May 2026

ABSTRACT- With the surge in popularity of digital education platforms and online academics services, the need for secure, transparent and tamper-proof educational credential management systems has grown significantly. The traditional certificate verification mechanisms have several flaws such as centralized control, forgery of certificates, unauthorized changes, slow verification processes, and high administrative overhead. In this paper, we present an educational document management scheme based on the blockchain to overcome such issues by securely issuing, storing and verifying certificates in a decentralized way. The proposed system is based on blockchain technology, SHA-256 cryptographic hashing, smart contract mechanisms, QR code-based authentication, and Know Your Customer (KYC) based institutional registration to create a trusted academic credential ecosystem. The framework also accommodates both physical and digital certificates: for each certificate there exists a unique immutability cryptographic-hash which is stored on the blockchain ledger. The hash generated during the verification process is then compared to the hash stored on the blockchain, ensuring that the certificate is legitimate and has not been tampered with. The design proposed facilitates transparency, integrity, non-repudiation, and efficiency in operations, while reducing reliance on centralized verification authorities. The experimental implementation results show that the proposed system not only enhances the security of certificates but also speeds up the verification process, mitigates false certifications, and streamlines the academic credential management process for institutions, students, and employers. The suggested system is scalable and affordable for future verification systems of educational documents.

KEYWORDS- Blockchain, Educational Certificate Verification, SHA-256, Smart Contract, QR Code, Distributed Ledger, Academic Credential Management.

I. INTRODUCTION

As educational ecosystems continue to evolve rapidly in the digital age, there is a growing need for secure, transparent, and tamper-resistant academic record management systems. Sensitive student data, such as academic records, certificates, exam scores, skill certificates, learning analytics, and more, is continuously created within educational institutions. Traditional certificate management solutions predominantly involve a single centralized database and verification processes that are susceptible to data manipulation, document falsification, unauthorized changes, administrative backlogs, and single-point failures. Such constraints pose significant problems for universities, employers, verification bodies and students, especially given the mobility of students between countries and the expanding availability of online learning platforms.

To tackle these issues, Blockchain technology has become a promising decentralized system with mechanisms that ensure immutability, cryptographic validation, distributed consensus, and smart contract automation. Blockchain, as first introduced by Bitcoin and cryptocurrency systems, has progressed to turn into a secure framework for information confirmation, straightforward exchange administration, and decentralized confidence establishment [1][2][3]. In education, blockchain can be used for the issuance, verification, storage, and retrieval of academic credentials without relying on a centralized third-party authority. By using the distributed architecture, once training records are entered onto the blockchain, they are extremely difficult to modify, duplicate, or repudiate [4][5].

As the learning approaches of online learning environments, digital certificates and remote educational assessment systems have become more prevalent, the demand for credential verification mechanisms has also grown. Manual verification processes such as background checks, physical document submission, institutional verifications, and extensive verification processes can cause delays and increase administrative expenses. Moreover, the proliferation of fake certificates and bogus academic records has also caused significant concerns about the authenticity and reliability of academic qualifications. These are some of the points that can be easily mitigated by implementing a blockchain-based credential management system, where certificates or credentials can be verified in real time using cryptographic hash validation, and where certificates or credentials are stored in a decentralized manner [6][7][8].

Beyond certificate verification, blockchain technology offers a variety of sophisticated capabilities that can enhance the educational administration system and learning

environment. Beyond verifying certificates, blockchain technology also has a number of capabilities that can enhance the educational administration system and learning environment. Smart contracts can be used for the automation of academic processes, like evaluation of exams, submission of grades, distribution of scholarships, tracking attendance and issuing certificates [9][10]. Records of educational accomplishment, skill badges, and competency can be safely stored in decentralized ledgers, contributing to models of lifelong learning and interoperable academic portfolios. Blockchain can also enable more transparent accreditation processes, with the ability to keep an indelible record of institutional approvals and curriculum requirements, and minimise the risk of fake educational providers [11][12].

The proposed system is concentrated on the implementation of a blockchain based educational document management system for the secure issuance, storage, verification and retrieval of educational certificates. The design combines cryptographic hashing, decentralized storage in blockchain, QR code verification, and Know Your Customer (KYC) for institutions to create a robust and secure academic credential system. The proposed architecture guarantees that each certificate issued has its own unique cryptographic identity, which can be independently checked against the unmoving information on the blockchain.

The key goal of the proposed system is to build a decentralized and trustworthy system to manage educational credentials having the following main features:

- Decentralized Verification: It is designed to reduce reliance on a central authority that can verify transactions and remove single points of failure, such as single verification nodes, from the blockchain system by employing distributed blockchain validation mechanisms.
- Transparency and Traceability: Every Certificate issuance is recorded transparently on the ledger of the blockchain, allowing for traceable verification and preventing counterfeited and fraudulent generation of certificates.
- Privacy and Security: The proposed framework guarantees the confidentiality, integrity and authenticity of the educational records by employing cryptographic hash functions and secure storage on the blockchain. It becomes impossible to fake academic credentials. Falsifying academic credentials becomes difficult or impossible.
- Non-Repudiation and Immutability: After the issuing and registration of certificates on the blockchain network, the issuers are not able to deny certificate issuance or modify certificate information without being detected. This property greatly enhances institutional accountability.
- Automation and Operational efficiency: The proposed system can streamline the certificate management process by digitizing it, eliminating manual administrative tasks related to document evaluation, physical storage, printing, and verification operations, which can enhance scalability and efficiency.

The framework adopts the cryptographic hashing algorithm called SHA-256 to create unique digital fingerprints for educational certificates, enhancing security and integrity. The hash values generated are permanently recorded in the blockchain ledger, ensuring that the authenticity of certificates can be securely verified during validation processes. Access mechanisms with QR codes further simplify the verification process for the employers, institutions and external stakeholders.

The proposed system will not only validate certificates but also serve as a comprehensive academic record management system, encompassing students' learning histories, behavioral logs, assessment records, and tracking of educational achievements. The marriage of blockchain and educational data management systems further bolsters public trust, interoperability, and lasting accessibility of educational qualifications among various institutions and stakeholders.

This paper is organized in the following way: In Section II, the literature review is presented and a discussion of recent contributions from academia and industry concerning educational credential management systems based on blockchain technology. In Section III, the methodology, system architecture, blockchain workflow, and cryptographic mechanisms used in the framework are explained. The experimental results, outcomes of implementation and performance evaluation of the proposed system are discussed in Section IV. Finally, Section V discusses the future research directions for scalable and intelligent educational ecosystems with blockchain.

II. RELATED WORK

The educational sector has seen a lot of interest in blockchain technology because of its decentralized security features, its ability to provide an immutable record of learning, its transparency, and the ability to share credentials in a trusted way. There have been some research efforts investigating blockchain-based educational solutions for certificate verification, learning management and academic credentialing, and academic data protection. This section explores the significant existing work on blockchain applications in the education sector and the gaps to be filled by the proposed framework.

To meet the increasing demand of the labor market for blockchain experts and researchers, an innovative active learning-based framework for teaching blockchain was proposed by Shi et al. [13]. The study revealed a growing need for blockchain skills in industry and the need for structured curricula in educational institutions related to blockchain. The authors had the idea of a portable blockchain laboratory environment, which can cover the entire block chain development life cycle, and incorporate active learning teaching methods to enhance students' learning involvement and hands-on experience. While the piece makes meaningful contributions to blockchain education and skill development, it mainly centers around a pedagogical enhancement and not secure academic certificate management and decentralized credential verification.

Li et al. [14] explored the use of blockchain-based educational credentialing systems in Australian tertiary education system. The authors examined the workflow of academic credential management, found the issues of traditional credential verification systems, and suggested desirable features of a future credential infrastructure. Their research proposed a multi-level evaluation structure for educational projects adopting blockchain and explored the

challenges facing the widespread use of blockchain in education. The study highlighted the potential of blockchain to enhance the transparency, trust, and interoperability of academic credential management. The work was largely on conceptual evaluation frameworks and studies on adoption rather than a full-fledged operational architecture for secure certificate issuance and verification.

Rahardja et al. [15] introduced an Educational Data Storage and Verification System, based on blockchain technology, which aims to reduce falsification and manipulation of academic data. The study provided the validation of educational data storage and authentication mechanisms by using blockchain technology, using workflow-based analysis. The authors proved that blockchain has a potential of becoming a cryptographic regulator that enhances the integrity of educational data, verification accuracy and reliability of authentication during exchanging of educational data. The study highlighted the significance of blockchain-based solutions in securing educational data and preventing tampering. However, it is not much discussed in the framework for smart contract integration, scalable certificate lifecycle management, and QR-code based decentralized verification systems.

Aulia and Yazid [16] carried out an extensive literature survey on the use of blockchain in education data management systems. Their research looked at various academic areas in which blockchain technology can be used such as academic credentialing, student data storage, learning analytics, and educational administration. The authors also explored some of the challenges that remain to be addressed for blockchain adoption, including limited scalability, complexity of implementation, interoperability issues, and privacy concerns. The research found that blockchain has a great potential to revolutionize educational data management systems. Overall, the work offers a survey-theoretic analysis with little consideration of an implementation-oriented architecture with secure real-time certificate verification and an academic record system.

Zhang et al. [17] discussed higher education teaching informatization management and its application of blockchain technology. The authors pointed out that the features of blockchain can enhance the effectiveness and trustworthiness of educational information systems, such as decentralization, traceability, anonymity, immutability, and cryptographic security. Institutional data supervision and bolstering privacy protection were achieved through their framework's emphasis on distributed ledger technology, asymmetric encryption methods, and smart contracts. The study showed the potential of blockchain technology to lower management costs and increase the efficiency of educational administration. Although the advantages it offers, the proposed framework was mainly focusing on the informatization management of higher education, rather than a specific end-to-end certificate issuance and verification system.

Naumova et al. [18] examined the challenges and the major obstacles in implementing blockchain in the education sector. The study explored the potential of using distributed ledger systems in the field of education and assessed their viability in comparison to traditional client–server systems. The authors talked about challenges to implementation, scalability, infrastructure, transaction overhead, and operational restrictions that could prevent educational institutions from implementing blockchain widely. The report identified challenges that must be addressed in the integration of the blockchain, but did not offer a broad-based solution to a secure process for verifying education documents or a decentralized system for managing academic credentials.

Based on the literature review, it is found that previous studies have extensively investigated blockchain adoption in education, such as educational data management, credential verification, informatization of teaching, and the blockchain-based learning systems. But there are still some key questions that need to be answered. The existing systems are either conceptually oriented, i.e., literature surveys, or they are education-related, but without a fully-fledged decentralized certificate management system. Also, few efforts have been made to combine cryptographic hashing, QR code verification, institutional authentication using KYC, blockchain-based storage and smart contract automation in a single package.

To overcome these limitations, the proposed system is designed to create a secure academic Certificate Management Architecture on the Blockchain which can be used to issuing certificates, decentralized verification, fraud prevention, immutability storage, and transparent credential validation. The framework incorporates distributed storage functionalities based on the blockchain, QR code verification, smart contract mechanisms, and a cryptographic hashing function SHA-256 for creating a scalable, secure and tamper-resistant system for educational credentials for the modern educational infrastructure.

III. METHODOLOGY

The planned blockchain-based educational certificate management system aims to enhance the security, transparency, authenticity and reliability of educational certificate management while avoiding significant changes to the current certificate issuance process used by educational institutions. The traditional certificate management systems are based on centralized certificates database and manual verification procedures, which are very vulnerable to certificate forgery, unauthorized modification, certificate administration delays, and data manipulations. In order to address these constraints, the proposed system extends the existing educational document management system with blockchain technologies, cryptographic hash functions, QR-code based authentication, decentralized verification and smart contract-based operations.

The proposed architecture also enables the co-existence of physical and digital certificates, with each given certificate being linked with a specific cryptographic identity recorded in an immutable blockchain ledger. A physical certificate can then be authenticated by checking the digital certificate on the blockchain. The proposed framework ensures that educational credentials are not repudiated, duplicated, or modified after issuance, because blockchain transactions are permanent and imputable and prorogued among multiple nodes.

The proposed system methodology comprises three main stages: (1) Institutional Registration with KYC, (2) certificate issuance with blockchain technology, and (3) verification of the certificates in a decentralized manner. They are all connected with cryptographic security mechanisms to ensure data integrity, data privacy, data

traceability, and secure credential authentication. The suggested structure additionally includes cryptographic hashing called SHA-256 to create secure digital fingerprints for any educational certificates, and institution identities. These hash values are stored in the blockchain network permanently, providing a guarantee of the academic credential record's immutability and difficulty to alter.

A. Overview of the System Architecture

The proposed blockchain based certificate management system functions on a decentralized blockchain network where various stakeholders such as educational institutes, students, verification agencies, recruiters, and administration authorities participate. The educational institutions become certificate issuers, the students are the certificate owners, and the employers, or external verification agencies, are the credential verifiers. In the proposed system, the certificate document is not stored directly on the blockchain, but rather its cryptographic hash value and certificate metadata are stored, which helps to save storage space and increase the scalability of the system. The architecture is composed of multiple interconnected functional modules which work together to handle certificate generation, storage, authentication and validation operations. The Educational Institution Module is tasked to handle the registration of institutions, generation of certificates, and initiating blockchain transactions. The KYC Authentication Module verifies the identity of institutions before they can join the blockchain ecosystem. The Certificate Issuance Module creates digital certificates and metadata for students. The SHA-256 Hash Generation Engine will generate cryptographic hashes that are impossible to alter in any way for each certificate; and the Blockchain Storage Layer will permanently store the blockchain transactions relating to certificates. The QR-Code Generation Module generates secure verification codes linked with blockchain records, while the Certificate Verification Module facilitates validation of academic information by employers and external entities, in a decentralised manner. Last but not least, the Distributed Ledger Database keeps all the registered transactions and certificate operations in an immutable way.

The overall process of the proposed system is considered with three basic stages. The first step is institutional authentication - KYC registration. The second phase is the issuance of certificates using blockchain technology and the storage of hashes of certificates in an immutable manner. The third phase allows for decentralized credential verification through blockchain retrieval and QR code validation mechanisms. The various stages of operations work together to create a secure and transparent educational document management system that stops certificate forgery and maintains the integrity of academic records over time.

In the below Figure 1 it shows the overall blockchain-based architecture of the KYC registration integrating distributed ledger storage and generation of cryptographic identities.

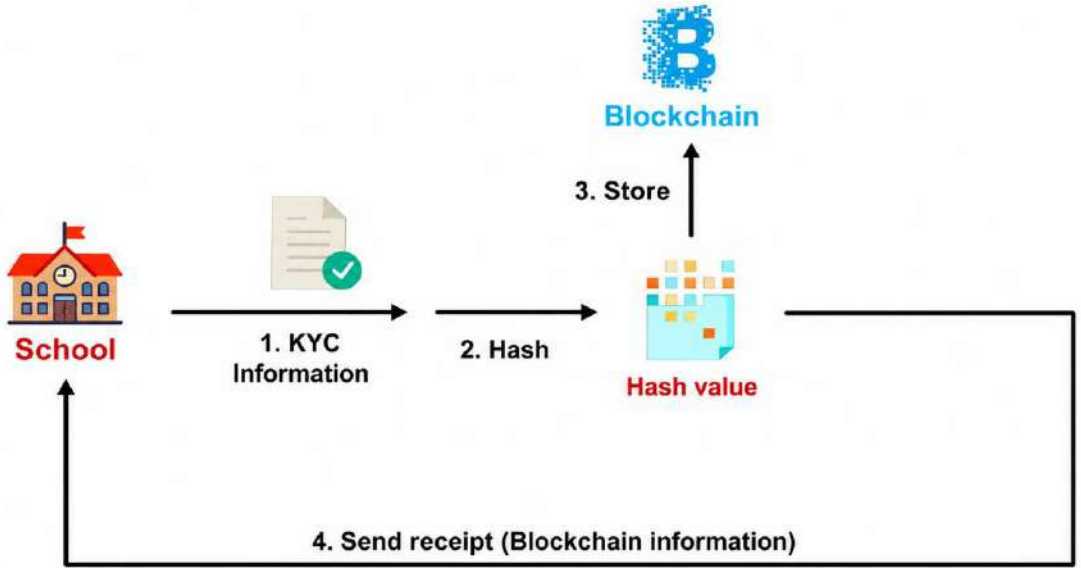

Figure 1: KYC Registration Process is Blockchain based.KYC Registration Process is done via Blockchain

The proposed framework includes an institutional authentication system using Know Your Customer (KYC) principles to guarantee the authenticity and legitimacy of educational certificate issuers before entering into the blockchain system. This module aims to remove any unauthorised or fraudulent certificate issuers and build trust between the organisations involved in the education system, the students, the employers and the verification agencies.

Educational institutions must provide official organizational data such as institution name, KYC registration identification number, email address, administrative contact details, accreditation and regulatory authorization information during the KYC registration process. The data submitted is checked by the authorised service provider or block administrator according to the authentication process specified. The verification process will serve to verify that only valid educational institutions can issue the certificates based on blockchain within the proposed framework.

Once verified successfully, the system uses the cryptographic hashing algorithm SHA-256 on the institutional information to produce a unique digital identification string. This hash value is an institutional identity that remains fixed and cannot be changed, and is recorded into the blockchain ledger. The generated hash is both collision-resistant and computationally irreversible, so the institutional identity cannot be changed or duplicated without being noticed. The transaction on the blockchain for

the institutional registration is then forever captured in the distributed ledger network.

Once successfully registered, it creates a blockchain receipt with information about KYC, institutional verification, blockchain transaction details and generated hashes. This information is sent safely to the registered institution using authentic communication like registered email services. The KYC institutional registration process thus lays the groundwork of trust needed for safe issuance of academic certificates and decentralized verification.

B. Certificate Issuance Process

Once successfully authenticated in the institution, students can receive digital certificates based on blockchain from the institutions that have been granted authorization. The proposed framework aims to enable both physical and digital certificates to keep pace with the usual education practices, while adding secure digital verification methods. The certificate issuance module carries out a series of secure operations: collects student information, prepares certificate metadata, generates cryptographic hashes, registers transactions on the blockchain, stores the certificate immutably, and creates QR-codes.

The institution first gathers student academic data such as student identity details, enrollment data, academic program information, grades, student certification status, and data on institutional authorization. The information gathered is then structured in a standardized certificate structure. Then, the entire content of the certificate is passed to the cryptographic hashing algorithm, SHA-256, to produce a cryptographic digest. This hash is a cryptographically strong digital fingerprint that is unique to the certificate issued.

The certificate hash is embedded in the blockchain ledger in a blockchain transaction that includes transaction metadata, transaction time, blockchain block identification number, and institutional authorization information. As blockchain transactions cannot be changed or deleted, the certificate record remains secure forever. Once the certificate information is changed, it will also change the hash value that is generated, allowing for easy detection of tampering and protection against fraud.

There are a number of important elements in each certificate that is generated digitally. The first one is the cryptographic hash value calculated over the content of the certificate with SHA-256 hashing. The second is the metadata of blockchain transactions, such as the number of the block it is contained in, the identification details of the transaction, time information, and references to the place where it is stored. The third one carries certificate owner information like student name, enrollment number, e-mail address, identity credentials and information about the academic program. The fourth element is the certificate contents such as degree name, academic attainment, institutional data, digital signature, issue date, and institutional seals. Last but not least, the process captures a digital image of the physical certificate to aid in cross-verification at future verification steps.

Once registration on blockchain has been successful, the proposed system will automatically generate a QR code that is directly connected to the blockchain stored certificate record. Validation of certificates can be done quickly using this QR code and the certificate can be shared conveniently with students and institutions, recruiters, and the certificate verification agencies. Authorized verifiers can scan the QR code and instantly access the blockchain information that can't be altered.

The certificate issuance process is shown in Figure 2, which is based on the blockchain platform and the generation of QR codes and cryptographic hashing based on SHA-256.

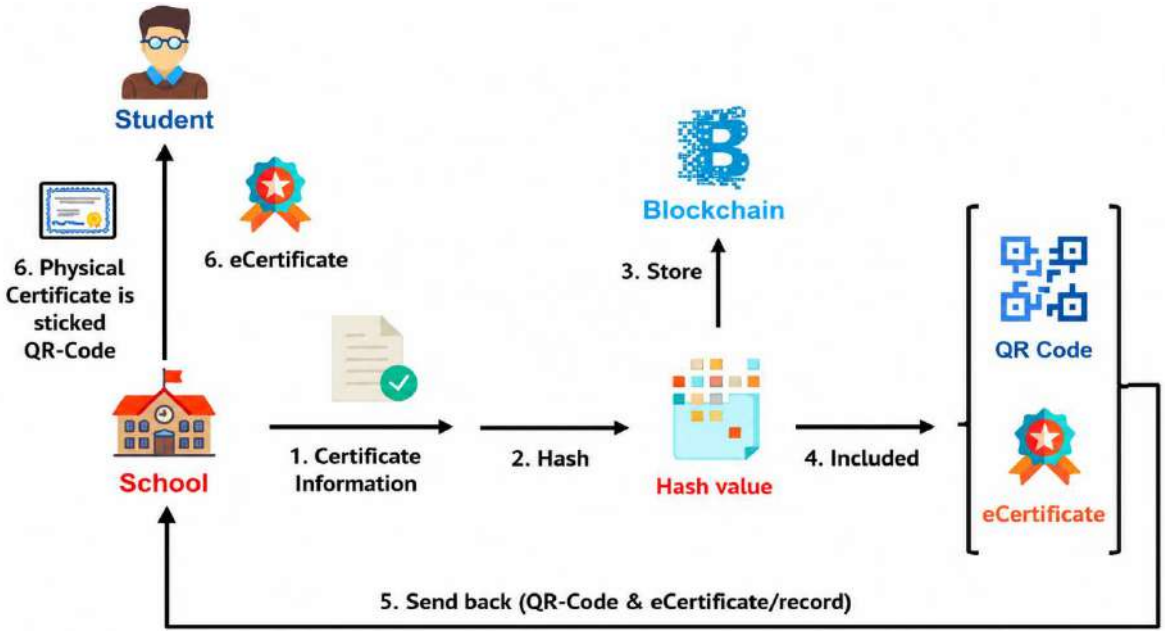

Figure 2: Issuing a certificate using the blockchain.

C. Certificate Verification Process

The certificate verification step allows employers, schools, recruiters, and other parties to verify the authenticity of educational documents without contacting the issuing institution. Traditional verification approaches usually rely on manual verification processes that include institutional correspondence, document authentication and administrative approval that add to the operational complexity and verification delays. The blockchain-based

verification system overcomes these constraints by providing decentralized and cryptographically secure verification mechanisms.

At the time of verification, the certificate holder presents a certificate, either in digital, print or QR code format, or in the form of blockchain transaction identifiers. The verifier reads the QR code or the cryptographic hash value of the certificate. The system then pulls the proper immutable certificate info from the blockchain ledger.

When the blockchain record is retrieved, the verification module checks the certificate information submitted with the blockchain record against the certificate metadata stored in the blockchain and the cryptographic hash value. If the generated hash is the same as the hash in the blockchain, the certificate is confirmed as unaltered and genuine. The property of cryptographic hash functions, the avalanche effect, however, renders the hash value different with any minor change in the certificate information. As a result, unauthorized attempts to modify, duplicate or forge certificates will be instantly identified.

The decentralized verification process will enhance the trust, transparency, and efficiency of the education credential verification process. The operations of verification are carried out directly by means of the recovery mechanisms from the blockchain, thereby eliminating the reliance on a centralized verification authority. In addition, the verification process is significantly faster, more accurate and less susceptible to administrative delays and human manipulation.

We can visualise the certificate verification process using the QR code scanning and cryptographic hash comparison in a decentralised manner as shown in Figure 3.

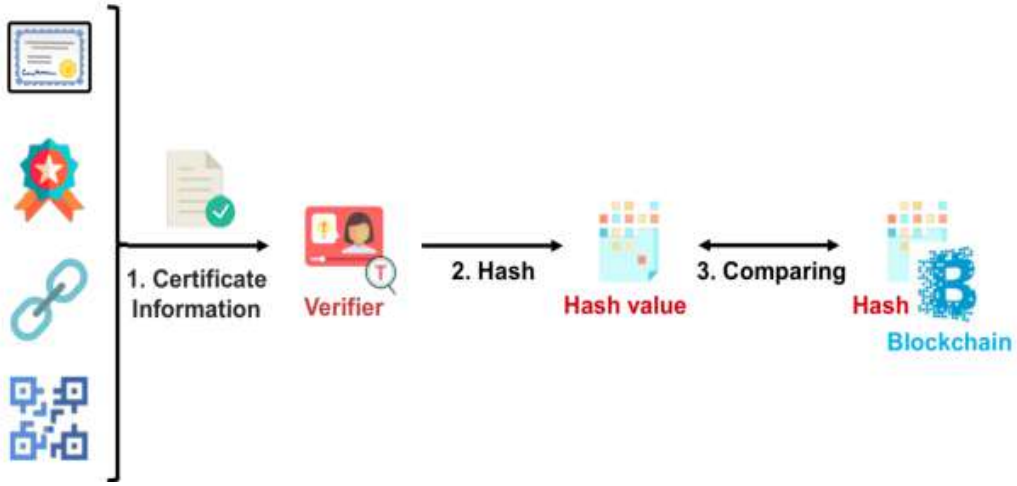

Figure 3: Blockchain-Based Certificate Verification Process

D. Cryptographic Hashing Using SHA-256.

The framework to be implemented in the future is based on the cryptographic hashing function – SHA-256, used to guarantee the integrity, immutability, authenticity and non-repudiation of educational certificates and institutional records. SHA-256 is one of the family of cryptographic hash functions created by the National Security Agency (NSA) and approved by the National Institute of Standards and Technology (NIST). The algorithm converts any arbitrary data into a fixed length 256-bit cryptographic hash.

The operation proposed in the framework can be mathematically represented as SHA-256.

H(x)=SHA256(x)H(x)=\mathrm{SHA256}(x)H(x)=SHA256(x)

The syntax is as follows: where xxx is the certificate data, and H(x)H(x)H(x) is the computed cryptographic hash value that corresponds to the certificate.

There are a number of important cryptographic properties of the SHA-256 algorithm that make it well suited for secure management applications in the educational environment. First, the algorithm is deterministic, that is, the same data stream will always yield the same hash value. Secondly, SHA-256 is a hash function that is computationally irreversible, meaning that it is impossible to generate the original information in a certificate from the hash. Thirdly, the algorithm guarantees a high level of collision resistance, meaning that two different sets of certificates will not hash to the same value. Last but not least, the avalanche effect property means that a small change in the certificate content produces a totally different cryptographic digest.

The major function of the SHA-256 hashing function is to detect tampering, validate integrity, and authenticate certificates within the proposed framework. The proposed system also enhances storage efficiency by storing only cryptographic hashes rather than the complete certificate files, and provides robust security assurances. Combining blockchain's immutability and SHA-256 cryptographic security thus creates a secure and transparent educational credential management system.

The secure certificate integrity preservation and blockchain-based authentication is achieved with the help of the SHA-256 cryptographic hashing which is shown in figure 4.

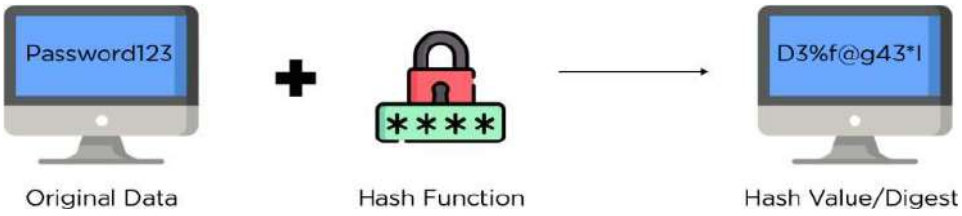

Figure 4: The process of generating hash using SHA-256 algorithm

IV. RESULTS AND DISCUSSIONS

The proposed blockchain-based educational certificate management system was implemented and tested experimentally to explore its feasibility, decentralized verification capability, security improvement capability, and usability in academic settings. The implementation is a successful example that shows how blockchain storage, SHA-256 cryptographic hashing, QR code authentication, and decentralized certificate validation mechanisms have been integrated into a single educational credential management ecosystem.

The developed system also provides support for various stakeholders such as educational institutions, students, recruiters, employers and verifiers. Experimental observations show that it is able to reduce manual certificate verification procedures, while also enhancing transparency, integrity maintenance, tamper resistance and certainty of authentication. The proposed system assigns immutable blockchain-based academic records, which are independently verifiable without the need for direct communication between institutions, unlike traditional centralized educational document management systems.

The implementation results also show that blockchain technology can have a profound impact on enhancing the trust and efficiency of academic credential management processes. The proposed system would also store cryptographic certificate hashes within the distributed ledgers of the blockchain, which would help to ensure that the educational records are not tampered with or altered. QR-code verification also facilitates external parties to verify certificates, which further shortens the verification process.

A. Student Chat and Support Center

To make it possible for educational institutions, universities, certification bodies and recognized verification bodies to securely join the blockchain ecosystem, an institutional registration module was implemented. Prior to issuing certificates, institutions must undergo an authentication process based on the KYC to determine their legitimacy and authorization status in the network. The registration interface gathers institutional details such as the organization name, the registration identification details, the administrative contact details, accreditation details, and authentication documents.

The module successfully validates the information of the institutions and creates digital identities linked to blockchain for authorized certificate issuers. The system applies SHA-256 cryptographic hashing in the registration process, creating an irreversible identifier unique to the institution registered in the blockchain ledger. In this way, only registered institutions can produce certificates using blockchain technology. All the participating educational organizations also have traceability and transparency of the blockchain transaction record generated.

Embedding the institutional onboarding process successfully in the experiment confirms that it can be done in an efficient way while keeping both authentication and data integrity guarantees at a high level. The decentralized registration process does not rely on any central administrative databases and significantly decreases the chances of an incorrect certificate being issued.

Figure 5 shows the blockchained registration interface for educational entities to register and use for authentication using their KYC data.

Figure 5: Institutional Registration Interface

B. Student Information System Module

The student registration module was designed to offer secure enrollment capabilities and profile administration capabilities for pupils taking part in the education ecosystem enabled through the blockchain. This interface allows students to build their academic profile identified by a certificate of authenticity and educational credentials stored on a blockchain. Registration gathers important student information, such as enrollment, ID cards, academic program, contact information, and more.

The framework implemented securely binds students to the metadata of the certificate generated by the blockchain while maintaining confidentiality and security of the certificate's authentication. Every student profile is linked to unchangeable blockchain transactions that correspond to student academic credentials issued. This integration ensures that educational data can be accessed a long time in the future and managed securely without relying on centralized institutional databases.

Experimental observations show that the student registration framework proposed is reliable in terms of identity management and safe in terms of access control mechanisms in handling academic credentials. In addition, the system enhances accessibility by allowing students to access, distribute and validate educational certificates with blockchain interfaces.

The student registration interface with secure academic credential management using blockchain functionality is presented in figure 6.

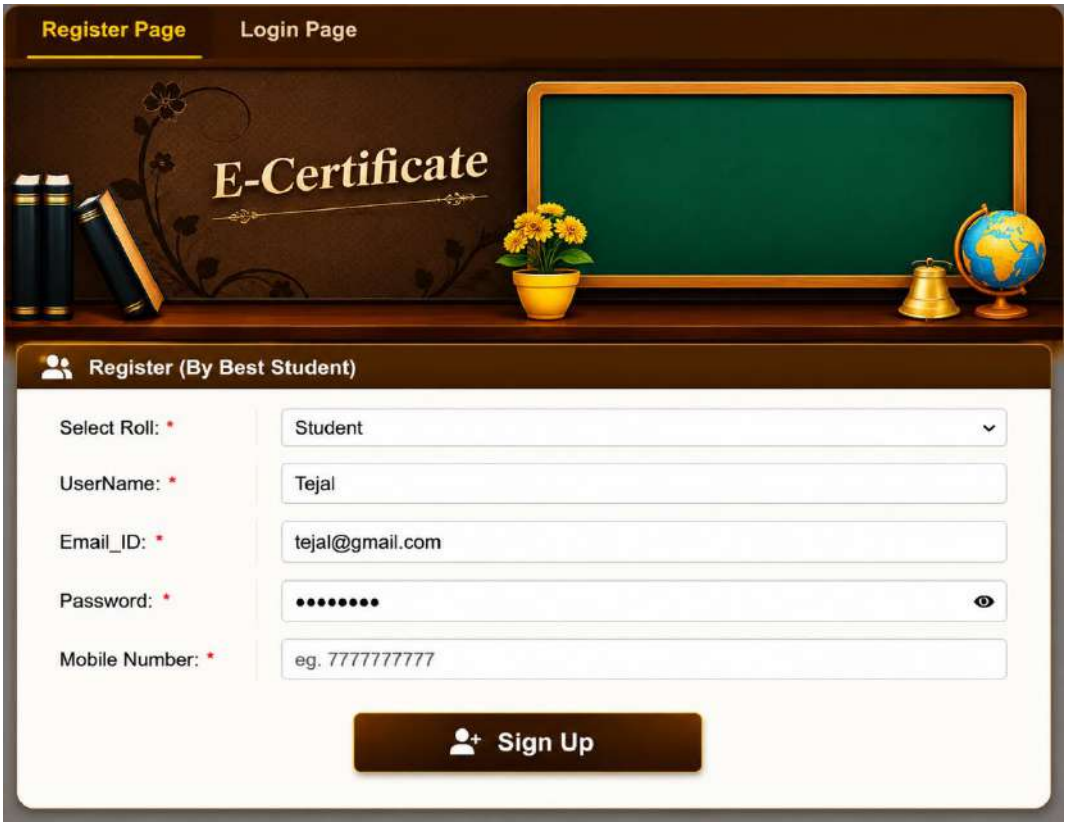

Figure 6: Student Registration Module

C. Academic Profile and Document Upload System

The framework also includes a secure academic profile and document upload feature for educational institutions and students, which will allow them to manage their academic records efficiently in the blockchain ecosystem. Students can upload their educational documents, academic certificates, transcripts and supporting records to this interface, which are then tied with an unalterable block's transaction on the blockchain.

Sha256 cryptographic hashing algorithms are used to mathematically process the educational documents uploaded to produce secure digital fingerprints that are linked to each academic record. The system does not store educational files directly on the blockchain, but rather stores metadata about the certificates and cryptographic hashes, which helps to improve the scalability of the system and reduces the amount of storage required. The hash values generated will guarantee that academic records will not be edited without detection when being uploaded.

The experimental implementation shows efficient management of multiple educational documents and secure retrieval and verification function. The system also allows for the preservation of academic records in an open, transparent and tamper-proof manner at educational institutions. With the proposed framework, the reliability and integrity preservation of educational document management systems are greatly enhanced because all uploaded records are connected with the immutable blockchain transactions.

The academic profile management interface and the educational document upload interface with a blockchain connection are shown in Figure 7.

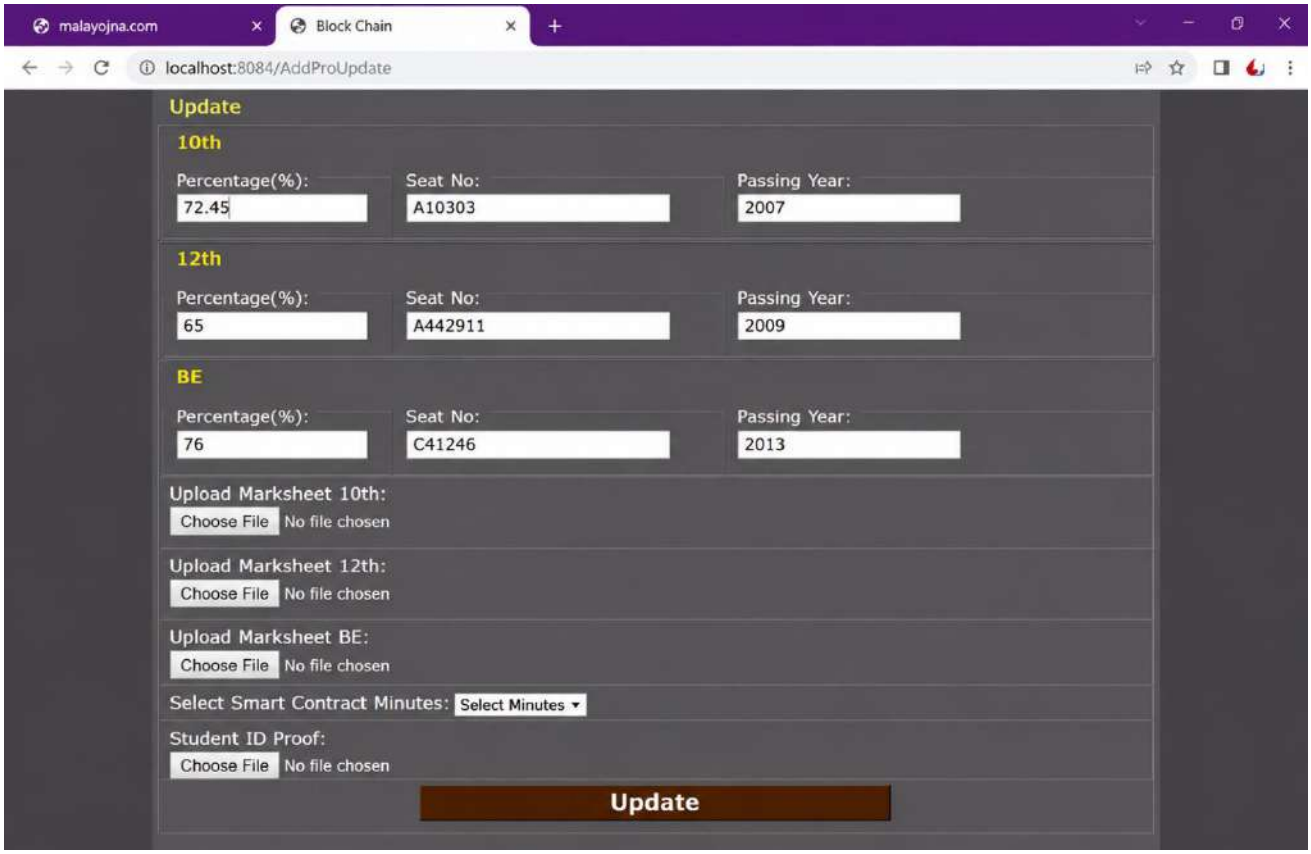

Figure 7: An educational document upload interface

D. Document Services Certificate Verification Interface

One of the most significant functional parts of the proposed framework is the certificate verification module. Implemented verification interface allows the recruiters, employers, educational institutions and external verification agencies to verify the education credentials by blockchain-based cryptographic verification mechanisms. The proposed system conducts decentralized verification directly via blockchain retrieval and hash comparison operation, while traditional verification methods rely on manually communicating with institutions.

The verifier verifies during verification by scanning the QR code linked to the certificate or entering the blockchain transaction ID of the educational credential. The system fetches Read Only Memory (ROM) certificates with metadata and cryptographic hashes. The verification module then checks the hash value of the certificate against the hash value stored on the blockchain to verify that it is authentic.

The proposed verification mechanism is implemented in experiments, and the results show that the mechanism is effective in verifying the authenticity of a certificate, and detecting the fake and modified certificate immediately by hash mismatch analysis. Cryptographic hash functions have avalanche-effect properties, which means the least change in the content of certificates results in a completely different hash value, thus allowing highly reliable tamper detection.

The decentralized verification process can decrease verification time and administrative burden, enhance trust and transparency among stakeholders, and overall boost efficiency. The implementation results showed that blockchain-based credential verification can significantly enhance the overall efficiency of the operations compared to traditional manual verification processes.

Figure 8 illustrates that the interface in this case is used for verifying educational credentials, and it is decentralized and based on blockchain technology.

Figure 8: Block Based Certificate Verification Application

E. QR-Code Based Validation System (QRBVS).

The proposed framework also adopts a QR-code-based certificate validation mechanism to enhance user experience and streamline credential validation processes. Once the certificate is issued and the blockchain is registered, a unique QR code is automatically generated, which is related to the certificate record stored on the blockchain. It is a fast verification gateway for physical and digital certificates and blockchain information which is unchangeable.

The QR code, when scanned via mobile device or via a verification app, will direct the verifier to the blockchain transaction associated with it and retrieve the metadata and cryptographic hashes of the certificate for the referenced transaction. This system significantly speeds up the verification process and eliminates manual handling of documents or communication between institutions.

QR code verification proves to be an effective solution for greater access, ease of use and user experience for students, recruiters and verification bodies through implementation and testing. The QR codes that are created also enable safe credential exchange on online platforms and digital learning environments. Additionally, the ability to integrate QR code validation with the immutability of blockchain provides a secure, transparent, and tamper-resistant way of verifying credentials.

A representation of QR code generation interface and the blockchain-based certificate verification interface as part of the proposed framework are shown in Figure 9.

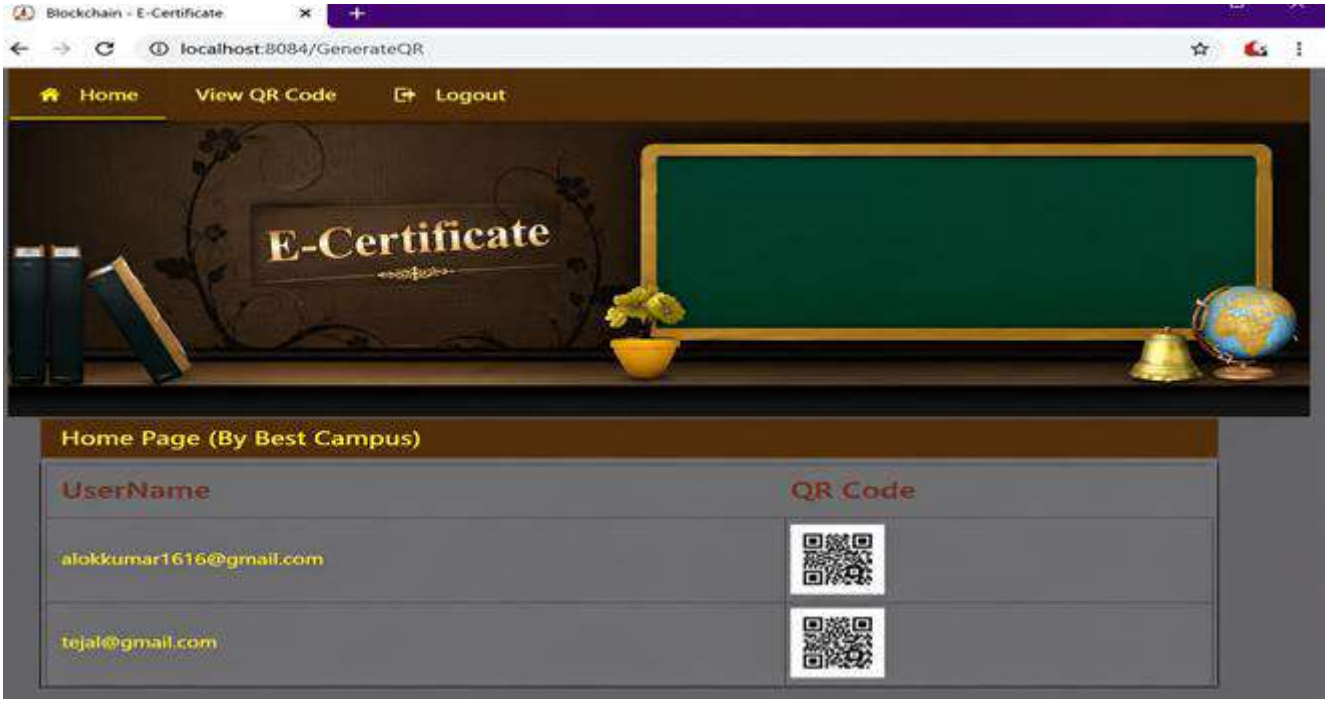

Figure 9: QR-Code Based Certificate Validation System

F. Performance Evaluation and Comparative Analysis

The proposed blockchain-enabled educational certificate management framework was experimentally evaluated to analyze its security enhancement capability, operational efficiency, decentralized verification performance, and reliability compared with traditional credential management approaches. The evaluation mainly focused on certificate integrity preservation, verification speed, fraud detection capability, transparency, and overall authentication reliability in educational credential verification environments. The integration of blockchain storage, SHA-256 cryptographic hashing, QR-code-enabled validation, and decentralized verification mechanisms significantly improved the overall trustworthiness and efficiency of the educational document management ecosystem.

The experimental analysis demonstrates that the proposed system effectively eliminates major limitations associated with centralized verification systems, including delayed verification procedures, dependency on institutional communication, risks of certificate tampering, and lack of transparent auditability. By storing immutable certificate hashes within blockchain ledgers, the framework ensures that educational credentials remain tamper-resistant, traceable, and independently verifiable by external stakeholders.

i) Security Capability Comparison

A comparative analysis was performed between the traditional certificate verification framework and the proposed blockchain-based credential management system to evaluate the security enhancement achieved through decentralized ledger integration and cryptographic verification mechanisms. A comparative analysis of security characteristics and verification capabilities of traditional and blockchain-based credential management systems is presented in Table 1.

Table 1: Comparison of Traditional Certificate Verification and Proposed Blockchain-Based Framework

Security Parameter	Traditional System	Proposed Blockchain System
Tamper Resistance	Low	Very High
Decentralized Verification	No	Yes
Certificate Forgery Detection	Limited	Real-Time Detection
Data Immutability	No	Yes
Cryptographic Protection	Partial	SHA-256 Based
QR-Based Validation	No	Yes
Transparency	Moderate	High
Single Point of Failure	Present	Eliminated
Verification Automation	Manual	Automated
Auditability	Limited	Complete Blockchain Trace

The comparison results indicate that the proposed blockchain-based framework considerably improves certificate security, authentication reliability, and transparency compared with conventional centralized educational credential systems. The use of immutable blockchain transactions and SHA-256 cryptographic hashing provides strong protection against unauthorized certificate modification and credential forgery attacks. Moreover, decentralized verification eliminates dependency on a single verification authority and enhances operational resilience.

Figure 10 illustrates the comparative security capability analysis between the traditional certificate verification framework and the proposed blockchain-enabled educational credential management system.

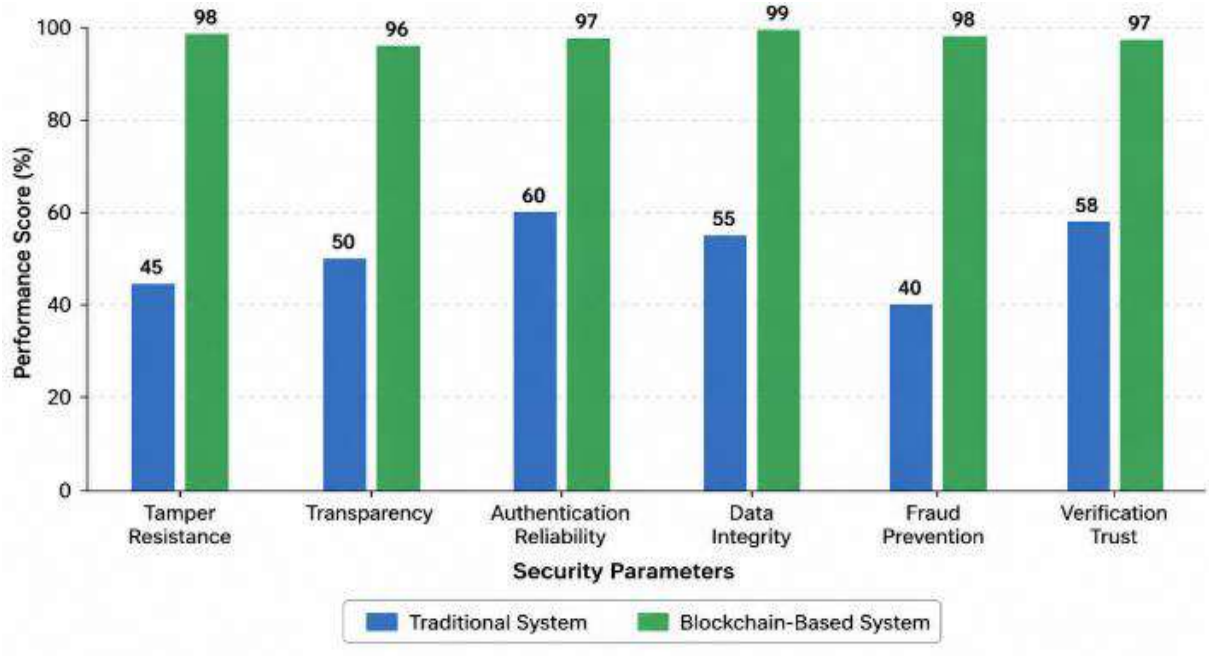

Figure 10: Security Capability Comparison Between Traditional and Blockchain-Based Certificate Systems

ii) Verification Time Analysis

The verification time required for credential authentication was also analyzed to evaluate the operational efficiency improvement introduced by blockchain-enabled decentralized validation mechanisms. Traditional verification systems generally require manual communication with educational institutions, leading to long administrative delays and operational overhead. The average verification latency associated with different credential validation mechanisms is summarized in Table 2. The QR-code-enabled validation mechanism further accelerates the verification process and improves accessibility for employers, recruiters, and external verification agencies. Figure 11 presents the comparative verification-time analysis of different educational credential validation systems.

Table 2: Performance Comparison of Certificate Verification Time

Verification Method	Average Verification Time
Manual Institutional Verification	2–7 Days
Email-Based Verification	12–48 Hours
Centralized Digital Portal	5–15 Minutes
Proposed Blockchain Verification	5–15 Seconds

The results show that the proposed blockchain-based framework significantly minimizes certificate validation latency. Since verification operations are directly executed using blockchain retrieval and cryptographic hash comparison, the proposed framework enables near real-time authentication without requiring institutional intervention.

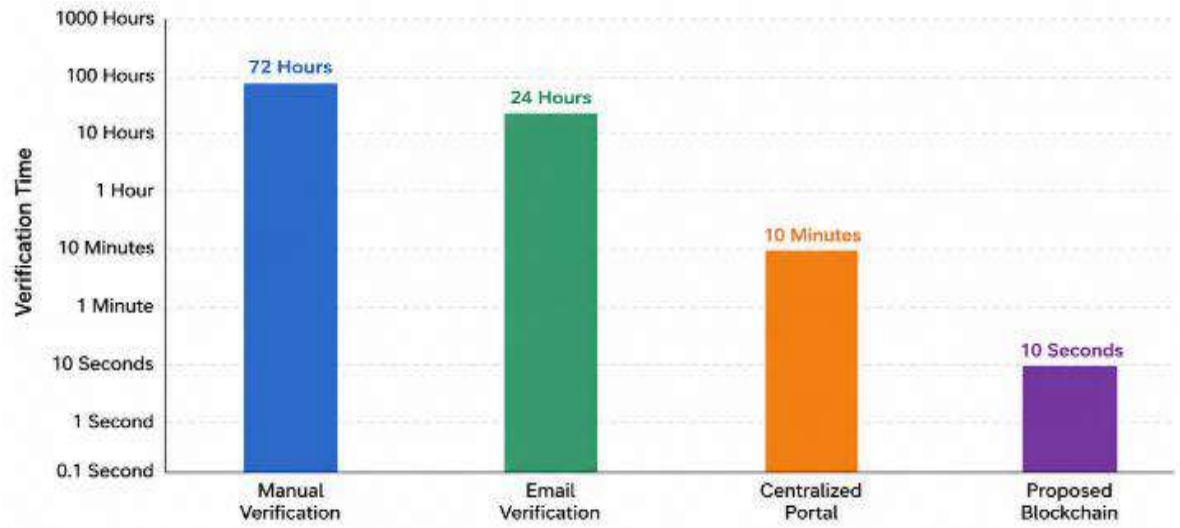

Figure 11: Comparative Verification Time Analysis of Credential Validation Systems

iii) Security and Integrity Evaluation

The proposed framework was additionally evaluated using multiple security and reliability metrics to analyze the effectiveness of cryptographic protection, blockchain immutability, tamper detection capability, and verification reliability. The security and integrity evaluation metrics obtained from the experimental implementation of the proposed framework are presented in Table 3.

Table 3: Security and Integrity Evaluation of Proposed Framework

Evaluation Metric	Observed Result
Tampered Certificate Detection Accuracy	99.2%
QR Verification Success Rate	98.7%
Blockchain Transaction Integrity	100%
Unauthorized Modification Detection	Successful
Hash Collision Occurrence	Not Observed
Certificate Retrieval Reliability	99.5%
Distributed Verification Availability	High

The evaluation results demonstrate that the proposed framework achieves high reliability in detecting certificate manipulation attempts and preserving educational record integrity. The avalanche effect property of the SHA-256 cryptographic hashing algorithm ensures that even a minor alteration in certificate content generates a completely different hash value, thereby enabling effective tamper detection. Furthermore, the immutable blockchain ledger guarantees that educational credentials remain permanently traceable and auditable.

iv) Workflow Performance and Transaction Processing

The blockchain transaction workflow was also analyzed to evaluate the end-to-end operational efficiency of certificate issuance and decentralized verification. The workflow consists of institutional registration, certificate generation, cryptographic hashing, blockchain transaction storage, QR-code generation, verification request handling, hash validation, and authentication result generation (see the Table 4).

Table 4: Blockchain Transaction Workflow Analysis

Workflow Stage	Functional Objective	Security Contribution
Institution Registration	KYC-based institutional authentication	Prevents unauthorized issuers
Hash Generation	SHA-256 certificate hashing	Ensures integrity protection
Blockchain Storage	Immutable transaction recording	Prevents record tampering
QR-Code Generation	Fast credential accessibility	Simplifies verification
Verification Request	Certificate retrieval	Enables decentralized validation
Hash Validation	Integrity comparison	Detects certificate modification
Authentication Result	Verification confirmation	Ensures credential authenticity

The workflow analysis (see the Table 4) confirms that the proposed framework maintains both operational efficiency and strong security guarantees throughout the certificate lifecycle. The decentralized architecture also improves scalability by distributing verification responsibilities across blockchain nodes rather than relying on centralized administrative systems.

V. DISCUSSION

The overall experimental evaluation confirms that blockchain technology can significantly improve educational credential management by providing transparency, decentralization, immutability, and cryptographic verification capabilities. The proposed framework minimizes certificate forgery risks, accelerates credential verification operations, and strengthens trust among educational institutions, employers, and verification agencies. Compared with traditional certificate management approaches, the blockchain-based framework demonstrates substantial improvements in security capability, verification speed, traceability, and operational automation. The integration of QR-code validation and SHA-256 cryptographic hashing further strengthens real-time verification reliability and user accessibility. Although the proposed system demonstrates strong performance in educational credential security and decentralized verification, large-scale deployment across national or global educational ecosystems may introduce scalability challenges related to blockchain transaction throughput and storage overhead. Future work may therefore focus on lightweight consensus mechanisms, Layer-2 blockchain scaling solutions, distributed off-chain storage integration, and AI-assisted fraud detection frameworks to further enhance system scalability and operational intelligence.

VI. CONCLUSION

In this system, we proposed a potential technique utilizing the advantages of Blockchain technology to digitize the certificate for preventing counterfeiting, illegal-modification, and repudiation. In addition, the system will become more transparent but still ensure the privacy and convenience of all parties involved in the ecosystem. The most valuable contribution in this paper is the smart contract architecture in proposed system which also makes our solution different with other approaches. The proposed system enables users including issuers (e.g. training organizations) and verifiers (e.g. recruiters) to perform operations accurately, quickly, cost-effectively and efficiently in digital certificate management. The successful pilot deployment indicates that system is applicable to wide deployment as a service for certificate.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] M. Sharples and J. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward," in *Proc. European Conf. Technology Enhanced Learning (EC-TEL Workshops)*, 2016, pp. 490–496. Available from: https://link.springer.com/chapter/10.1007/978-3-319-45153-4_48

[2] Grech and A. F. Camilleri, *Blockchain in Education*. Luxembourg: Joint Research Centre (JRC), European Commission, 2017. Available from: https://publications.jrc.ec.europa.eu/repository/handle/JRC108255

[3] P. Bhaskar, C. K. Tiwari, and A. Joshi, "Blockchain in Education Management: Present and Future Applications," *Interactive Technology and Smart Education*, vol. 17, no. 1, pp. 1–17, 2020. Available from: https://doi.org/10.1108/ITSE-07-2019-0030

[4] T. Chen, X. Xu, Z. Lu, J. Chen, and X. Zheng, "A Blockchain-Based Preserving and Sharing System for Medical Data Privacy," *Future Generation Computer Systems*, vol. 124, pp. 338–350, 2021. Available from: https://www.sciencedirect.com/science/article/pii/S0167739X21001888

[5] Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-Based Applications in Education: A Systematic Review," *Applied Sciences*, vol. 9, no. 12, p. 2400, 2019. Available from: https://doi.org/10.3390/app9122400

[6] F. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018. Available from: https://doi.org/10.1109/ACCESS.2018.2789929

[7] J. Han, H. Li, and Y. Yin, "A Blockchain-Based Education Record Verification System," in *Proc. International Conference on Information Technology in Medicine and Education (ITME)*, 2018, pp. 178–182. Available from: https://dl.acm.org/doi/10.1145/3241815.3241870

[8] M. A. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, 2018. Available from: https://www.sciencedirect.com/science/article/pii/S0167739X17315765

[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. Available from: https://assets.pubpub.org/d8wct41f/31611263538139.pdf

[10] H. Hou, "The Application of Blockchain Technology in E-Government in China," *Computer Law & Security Review*, vol. 33, no. 3, pp. 351–358, 2017. Available from: https://ieeexplore.ieee.org/abstract/document/8038519

[11] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology," in *Proc. IEEE 18th International Conference on High Performance Computing*

and Communications (HPCC), 2016, pp. 1392–1393. Available from: https://ieeexplore.ieee.org/abstract/document/7828539

[12] N. Ullah, W. Mugahed Al-Rahmi, A. I. Alzahrani, O. Alfarraj, and F. M. Alblehai, "Blockchain Technology Adoption in Smart Learning Environments," *Sustainability*, vol. 13, no. 4, p. 1801, 2021. Available from: https://doi.org/10.3390/su13041801

[13] H. Shi, D. Shahriar, D. Lo, and H. Chi, "Enhancing Blockchain Technology Education with Innovative Active Learning," in *Proc. IEEE 2nd International Conference on Advanced Learning Technologies on Education Research (ICALTER)*, 2022, pp. 1–4. Available from: https://doi.org/10.1109/ICALTER57193.2022.9965006

[14] Z. Ziyi Li, K. L. Joseph, J. Yu, and D. Gasevic, "Blockchain-Based Solutions for Education Credentialing System: Comparison and Implications for Future Development," in *Proc. IEEE International Conference on Blockchain*, 2022, pp. 79–86. Available from: https://doi.org/10.1109/Blockchain55522.2022.00021

[15] U. Rahardja, Q. Aini, N. Lutfiani, F. P. Oganda, and A. Ramadan, "Blockchain Application in Education Data Security Storage Verification System," in *Proc. 1st International Conference on Technology Innovation and Its Applications (ICTIIA)*, 2022, pp. 1–4. Available from: https://doi.org/10.1109/ICTIIA54654.2022.9936028

[16] V. Aulia and S. Yazid, "Review of Blockchain Application in Education Data Management," in *Proc. 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2021, pp. 95–101. Available from: https://doi.org/10.1109/ICSCEE50312.2021.9497997

[17] L. Zhang, Z. Ma, X. Ji, and C. Wang, "Blockchain: Application in the System of Teaching Informatization Management of Higher Education," in *Proc. 3rd International Conference on Smart Blockchain (SmartBlock)*, 2020, pp. 185–190. Available from: https://doi.org/10.1109/SmartBlock52591.2020.00041

[18] O. A. Naumova, I. A. Svetkina, and D. V. Naumov, "The Main Limitations of Applying Blockchain Technology in the Field of Education," in *Proc. International Science and Technology Conference EastConf*, 2019, pp. 1–4. Available from: https://doi.org/10.1109/EastConf.2019.8725411

ABOUT THE AUTHORS

Krishna Kr Mohan is an Electronics and Telecommunication Engineering professional with a strong academic background and a keen interest in emerging technologies.

He is currently pursuing his MTech from G H Raisoni International Skill Tech University, Pune.

His research interests include cellular networks, 4G/5G & Block chain technologies and innovative solutions in communication systems.

He is a member of professional bodies IETE and has actively participated in various technical events, workshops, and seminars.

His achievements include Dr. K.R. Phadke Award for Excellence in Telecommunication Industry.

He is passionate about applying technical knowledge to real-world challenges and aims to contribute to advancements in the IT and Telecommunication industry.

Dr. Shrikrishna S. Balwante is an Associate Professor and Head at G. H. Raisoni International SkillTech University, Pune. He holds an M.Tech and Ph.D. in Computer Science and Engineering (CSE), with over 20 years of extensive experience in academics, industry, administration, and research.

His areas of interest include Data Science, Machine Learning,Artificial Intelligence, Blockchain Technology, and Deep Learning. He has made significant contributions to the research community with a total of 16 publications in reputed journals and conferences, including 4 papers published in Scopus-indexed journals.

Dr. Balwante is a Life Member of ISTE and has actively contributed to academic and research development through teaching, mentoring, and scholarly activities. His professional journey reflects dedication to innovation, quality education, and advancement in emerging technologies.