Mr. Ankit Dhakane, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

A Hybrid On-Chain and Off-Chain Architecture for Academic Certificate Validation

Mr. Ankit Dhakane[1], Mr. Chetan Maurya[2], Dr.Jasbir Kaur[3],
Assistant Professor Ms. Sandhya Thakkar[4], Assistant Professor Mr. Suraj Kanal[5]

[1,2]Master of Computer Applications (MCA) at Guru Nanak Institute of Management Studies, Matunga, Mumbai, India
[3]Director & Head of Information Technology and HR at Guru Nanak Institute of Management Studies, Matunga, Mumbai, India
Guru Nanak Institute of Management Studies, Matunga, Mumbai, India[4,5]

Abstract- The rapid growth of digital education and online credentialing has increased the need for secure and efficient academic certificate verification systems. Traditional verification methods are often centralized, time-consuming, vulnerable to forgery, and dependent on manual institutional processes. Blockchain technology offers a decentralized and tamper-resistant solution for managing academic credentials. This research paper proposes a hybrid on-chain and off-chain architecture for academic certificate validation using blockchain technology and analyzes existing blockchain-based credential verification frameworks such as MIT Blockcerts. The paper examines the architecture, working mechanism, security features, and verification process of Blockcerts, along with its role in preventing certificate fraud and improving transparency. A comparative analysis of traditional and blockchain-based verification systems is also presented to evaluate efficiency, security, and scalability. The findings indicate that blockchain-based academic credential systems enhance trust, reduce verification time, and provide secure ownership of digital certificates. However, challenges such as scalability, interoperability, privacy concerns, and institutional adoption remain significant considerations for large-scale implementation. The study concludes that blockchain technology has strong potential to transform academic certificate management and verification systems in modern educational institutions.

Keywords: Blockchain, Academic Certificate Validation, Blockcerts, Digital Diploma, MIT, Certificate Verification, Educational Credentials, Distributed Ledger Technology, Cryptographic Hashing, Smart Contracts.

I. INTRODUCTION

The rapid digital transformation of educational institutions has increased the demand for secure, efficient, and globally accessible academic credential verification systems. Traditional certificate verification methods primarily rely on centralized databases and manual institutional validation processes, which are often time-consuming, expensive, and vulnerable to document forgery and tampering [5], [7]. The increasing number of fake academic certificates and fraudulent qualifications has become a major concern for universities, employers, and government organizations worldwide [8], [9].

Blockchain technology has emerged as a promising solution for addressing these challenges due to its decentralized, immutable, and transparent nature. Blockchain enables secure storage and verification of digital records using cryptographic hashing and distributed ledger mechanisms, thereby reducing

the possibility of unauthorized modifications and credential fraud [4], [6]. Several researchers have proposed blockchain-based frameworks for educational certificate validation to improve trust, transparency, and verification efficiency [4], [8].

One of the most significant practical implementations of blockchain in education was introduced by the Massachusetts Institute of Technology (MIT), which launched a blockchain-based digital diploma system using the Blockcerts framework [3].

MIT's initiative allowed graduates to receive tamper-proof digital diplomas that could be securely shared and independently verified without relying on centralized institutional verification [10], [11]. The system aimed to provide students with ownership of their academic credentials while simplifying verification processes for employers and educational institutions [2], [3].

The concept of digital credentials has also gained importance in modern online learning environments. MIT Open Learning emphasized the importance of bridging the "last mile" between educational achievement and employment by providing verifiable digital credentials that improve skill recognition and employability [1]. Blockchain-based credential systems support this vision by enabling trusted and portable academic records that can be instantly verified across organizations and geographic boundaries [5], [7].

This research paper focuses on designing a hybrid on-chain and off-chain architecture for academic certificate validation using blockchain technology. Existing frameworks such as MIT Blockcerts are analyzed to understand secure digital credential verification mechanisms and decentralized certificate management systems.

The study examines the architecture, working mechanism, advantages, limitations, and security aspects of blockchain-based credential verification. In addition, the paper analyzes existing literature related to blockchain-powered academic certificate systems and evaluates how such technologies can improve transparency, authenticity, and efficiency in educational credential management.

II. LITERATURE REVIEW

Traditional Certificate Verification Systems

Traditional academic certificate verification systems primarily depend on centralized institutional databases and manual verification procedures. Educational institutions usually issue physical certificates or digitally stored records that require direct verification through university authorities. These systems are often slow, resource-intensive, and vulnerable to forgery, duplication, and unauthorized modifications [5], [7]. Employers and organizations may experience delays during recruitment due to lengthy verification processes, especially when verifying international credentials.

Furthermore, centralized systems create a single point of failure, increasing the risk of data breaches and manipulation [9]. The growing incidents of fake academic certificates have highlighted the limitations of traditional verification mechanisms and created the need for more secure and transparent solutions.

Traditional academic certificate verification systems primarily depend on centralized institutional databases and manual verification procedures. Educational institutions usually issue physical certificates or digitally stored records that require direct verification through university authorities. These systems are often slow, resource-intensive, and vulnerable to forgery, duplication, and unauthorized modifications [5], [7].

Employers and organizations may experience delays during recruitment due to lengthy verification processes, especially when verifying international credentials. Furthermore, centralized systems create a single point of failure, increasing the risk of data breaches and manipulation [9]. The growing incidents of fake academic certificates have highlighted the limitations of traditional verification mechanisms and created the need for more secure and transparent solutions.

Blockchain Technology in Education

Blockchain technology has emerged as a secure and decentralized approach for managing educational records and digital credentials. Blockchain uses distributed ledger technology and cryptographic hashing to ensure data integrity, immutability, and transparency [4], [6].

In educational applications, blockchain enables institutions to issue tamper-proof digital certificates that can be independently verified without relying on centralized authorities.

Researchers have identified several advantages of blockchain-based academic systems, including faster verification, reduced fraud, improved transparency, and secure ownership of credentials [5], [8]. Smart contracts and decentralized storage mechanisms further enhance automation and trust within educational ecosystems. As a result, blockchain technology is increasingly being explored as a transformative solution for modern academic credential management systems.

MIT Blockcerts Framework

The Massachusetts Institute of Technology (MIT) introduced one of the earliest practical implementations of blockchain-based academic credential verification through the Blockcerts framework [3]. Blockcerts is an open standard for creating, issuing, storing, and verifying blockchain-based digital certificates [10].

The framework allows educational institutions to provide graduates with digitally signed and cryptographically secured academic credentials that can be independently verified using blockchain networks [11]. MIT's digital diploma initiative demonstrated how blockchain technology can improve certificate authenticity, portability, and verification efficiency while giving students ownership of their credentials [2], [3].

The Blockcerts framework also promotes interoperability and open-source adoption, enabling institutions worldwide to implement secure digital credential systems.

Review of Existing Research Papers

Several research studies have explored the application of blockchain technology for academic certificate verification and validation. Existing literature highlights the effectiveness of blockchain in preventing certificate fraud, improving verification speed, and ensuring data immutability [4], [6], [8]. Researchers have proposed various blockchain architectures, including public and private blockchain systems, smart contract-based frameworks, and decentralized verification platforms [7], [9].

Many studies emphasize the role of cryptographic hashing and distributed ledger technology in enhancing trust and transparency within educational institutions [5]. Additionally, practical implementations such as MIT's Blockcerts project have demonstrated the real-world feasibility of blockchain-based credential systems [10], [11]. The reviewed literature collectively supports the potential of blockchain technology in modernizing academic verification processes.

Research Gap Analysis

Although existing research demonstrates the advantages of blockchain-based certificate verification systems, several challenges and research gaps still remain. Many proposed systems focus primarily on conceptual models and lack large-scale real-world implementation and performance evaluation [8]. Issues related to scalability, interoperability between institutions, storage overhead, and privacy protection continue to limit widespread adoption [4], [6].

Furthermore, the integration of blockchain systems with existing educational infrastructure remains technically complex and costly for many institutions [7]. Limited research has also been conducted on user adoption, regulatory compliance, and standardization of blockchain-based academic credential systems. Therefore, further investigation is required to develop scalable, secure, and universally accepted blockchain frameworks for educational certificate validation.

III. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Introduction to Blockchain

Blockchain is a decentralized distributed ledger technology that securely records and stores data across multiple interconnected systems. Unlike traditional centralized databases, blockchain operates through a network of nodes where each participant maintains a copy of the ledger [6]. Data stored on blockchain is organized into blocks that are linked together using cryptographic techniques, forming a secure chain of records.

Once information is added to the blockchain, it becomes extremely difficult to modify or delete, ensuring data integrity and transparency [5]. Blockchain technology was initially introduced for cryptocurrencies such as Bitcoin, but its applications have expanded into several domains including healthcare, finance, supply chain management, and education [3]. In academic credential systems, blockchain enables secure issuance and verification of digital certificates without relying entirely on centralized authorities.

Key Features of Blockchain

Blockchain technology provides several important features that make it suitable for secure academic certificate verification systems. One of the primary features is decentralization, where data is distributed across multiple nodes instead of being controlled by a single authority [7]. Another significant feature is immutability, which ensures that once data is recorded on the blockchain, it cannot be altered without network consensus. Transparency is also an important characteristic, as blockchain transactions can be verified and audited by authorized participants [4]. Cryptographic security mechanisms protect the integrity and authenticity of stored records, reducing the possibility of tampering and fraud [9].

Additionally, blockchain systems offer traceability and reliability, enabling secure verification of digital credentials across organizations and geographic boundaries. These features collectively enhance trust and security within educational credential management systems.

Cryptographic Hashing

Cryptographic hashing is a fundamental component of blockchain technology that ensures data integrity and security. A hash function converts input data into a fixed-length encrypted output called a hash value or digital fingerprint. Even a small modification in the original data generates a completely different hash value, making tampering easily detectable [6].

Blockchain systems use cryptographic hashing algorithms such as SHA-256 to securely link blocks together and protect stored information from unauthorized changes [5]. In academic certificate verification systems, cryptographic hashing is used to create unique identifiers for digital certificates, ensuring authenticity and preventing duplication or manipulation. Hashing also enables efficient verification processes without exposing sensitive certificate data directly on the blockchain network.

Smart Contract Workflow for Academic Certificate Validation

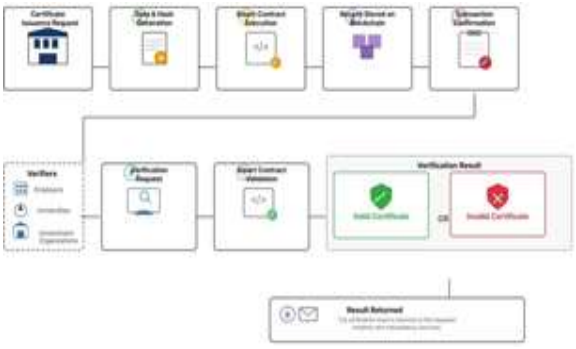

Fig. 1. Smart Contract Workflow for Academic Certificate Validation.

Smart Contracts

Smart contracts are self-executing digital agreements stored on blockchain networks that automatically perform predefined actions when specified conditions are met. These contracts eliminate the need for intermediaries by enabling automated and secure transaction processing [8]. In blockchain-based educational systems, smart contracts can automate certificate issuance,

validation, and verification processes. For example, educational institutions can issue digital certificates through smart contracts, while employers can instantly verify credential authenticity without contacting the issuing authority [6]. Smart contracts also improve efficiency, reduce administrative workload, and enhance transparency within academic verification systems. Their integration with blockchain technology supports secure and reliable automation of educational credential management processes.

Public vs Private Blockchain

Blockchain networks are generally categorized into public and private blockchains based on accessibility and control mechanisms. Public blockchains are decentralized networks that allow anyone to participate, validate transactions, and access records. Examples include Bitcoin and Ethereum networks [3]. These systems provide high transparency and security but may face scalability and transaction speed limitations. In contrast, private blockchains are controlled by specific organizations or authorized participants and restrict access to selected users [4].

Private blockchain systems offer better performance, enhanced privacy, and greater control over data management, making them suitable for institutional applications such as academic certificate verification. Educational institutions may choose either public or private blockchain models depending on factors such as scalability, security requirements, operational costs, and privacy considerations.

IV. HYBRID BLOCKCHAIN-BASED ACADEMIC CERTIFICATE VALIDATION ARCHITECTURE

Proposed Hybrid Architecture

Blockcerts is an open-source blockchain-based framework developed through collaboration between the Massachusetts Institute of Technology (MIT) and Learning Machine for issuing and verifying digital academic credentials [10]. The framework was designed to provide secure, tamper-proof, and independently verifiable digital certificates using blockchain technology. MIT became one of the first educational institutions to implement blockchain-powered digital diplomas through the Blockcerts system [3]. Unlike traditional paper-based certificates, Blockcerts enables students to securely store and share digital credentials while maintaining ownership and control over their academic records [11]. The framework uses cryptographic signatures and blockchain anchoring mechanisms to ensure authenticity, transparency, and protection against certificate fraud.

System Architecture

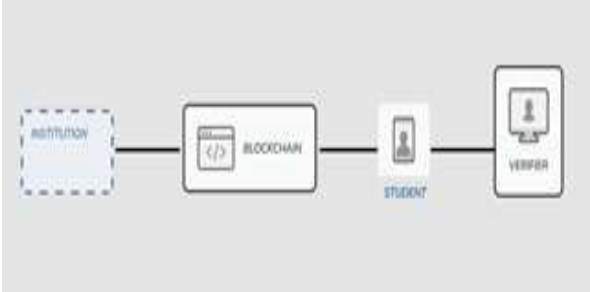

Fig. 1. System Architecture of MIT Blockcerts-Based Digital Diploma Framework (High level diagram)

The MIT Blockcerts-based digital diploma system consists of several interconnected components that work together to issue and verify academic credentials securely. The primary entities in the architecture include the issuing institution, blockchain network, certificate recipient, and verification platform [10]. Educational institutions generate digital certificates containing student information and cryptographic signatures.

These certificates are then hashed and anchored onto blockchain networks such as Bitcoin to create immutable verification records [3]. Students receive digital certificates through compatible applications or digital wallets that allow secure storage and sharing. Verification platforms access blockchain records to validate certificate authenticity without requiring direct communication with the issuing institution [11]. This decentralized architecture enhances security, transparency, and efficiency in academic credential management.

The proposed system follows a hybrid on-chain and off-chain storage architecture to improve scalability, efficiency, and security. Sensitive academic documents such as PDF certificates, student details, and metadata are stored off-chain in secure databases or cloud storage systems, while cryptographic hashes, transaction identifiers, and verification proofs are stored on-chain using blockchain technology. This hybrid approach reduces blockchain storage overhead and transaction costs while maintaining data integrity, transparency, and tamper resistance. During certificate verification, the uploaded certificate hash is compared with the corresponding blockchain record to validate authenticity and detect unauthorized modifications.

TABLE I: ON-CHAIN VS OFF-CHAIN STORAGE COMPONENTS

On-Chain Components	Off-Chain Components
Certificate Hash	PDF Certificate File
Transaction ID	Student Personal Information
Verification Proof	Academic Metadata
Smart Contract Records	University DatabaseRecords
Timestamp Information	Certificate Images and Attachments
Blockchain Verification	Cloud/Local Storage Systems

Workflow Mechanism

The working mechanism of the Blockcerts system involves certificate creation, blockchain anchoring, storage, and verification processes. Initially, the issuing institution generates a digital certificate containing academic information and applies a cryptographic digital signature [10]. A unique hash value of the certificate is created using cryptographic hashing algorithms and recorded on the blockchain network [5]. The original certificate is then shared with the student in digital format, while the blockchain stores only the verification proof rather than the complete certificate data. During verification, the system recalculates the certificate hash and compares it with the blockchain record to confirm authenticity and integrity [6]. Since blockchain records are immutable, any modification to the certificate immediately invalidates the verification process, thereby preventing forgery and unauthorized alterations.

On-Chain Certificate Issuance

The certificate issuance process in the MIT Blockcerts framework begins when an educational institution creates a digital academic credential for a student. The certificate includes details such as student name, degree information, institution details, and issue date [3]. The institution digitally signs the certificate using cryptographic keys to establish authenticity and ownership [10].

A cryptographic hash of the certificate is generated and anchored onto the blockchain network, creating a permanent and tamper-resistant verification record [11]. The finalized digital certificate is then delivered to the student through a digital wallet or certificate management application. Students can securely store, manage, and share these credentials electronically without depending entirely on physical documents or centralized databases.

Off-Chain Verification Process

The certificate verification process in the Blockcerts system allows employers, universities, and organizations to independently verify academic credentials without contacting the issuing institution directly. During verification, the verifier uploads or accesses the digital certificate through a compatible verification platform [10].

The system extracts the certificate hash and compares it with the corresponding blockchain record to validate authenticity and integrity [6]. If the generated hash matches the blockchain entry and the digital signature is valid, the certificate is confirmed as authentic [5]. Since blockchain records cannot be modified without consensus, the system effectively prevents tampering and fake certificate generation. This decentralized verification process improves efficiency, reduces administrative workload, and enhances trust in digital academic credentials.

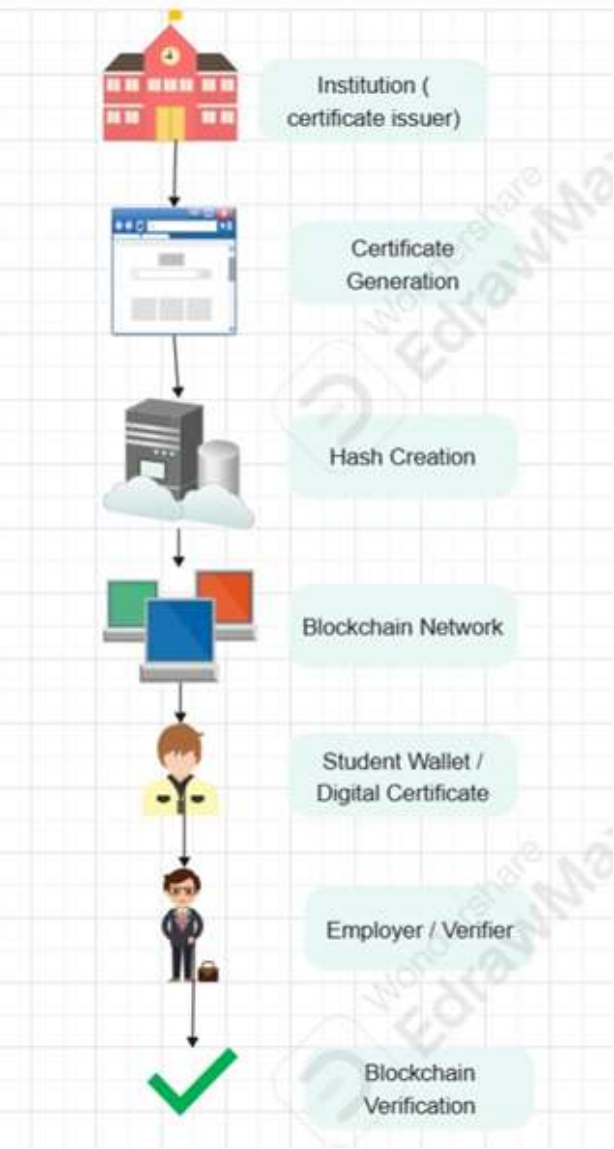

Fig. 2. Low level process architecture of the Blockcerts-based verification system.

V. RESEARCH METHODOLOGY

Research Design

This research adopts a qualitative and analytical research design to study the implementation of blockchain technology for academic certificate validation using a hybrid blockchain-based certificate validation architecture inspired by existing frameworks such as MIT Blockcerts. The study focuses on understanding the architecture, working mechanism, advantages, limitations, and security aspects of blockchain-powered credential verification systems. A comparative approach is used to analyze traditional certificate verification methods alongside blockchain-based solutions [4], [7]. The research also examines existing literature, technical reports,

and institutional implementations related to digital academic credentials and blockchain technology. This design enables systematic evaluation of the effectiveness and practicality of blockchain-based academic verification frameworks.

Data Collection Methods

The data used in this research was collected primarily from secondary sources, including research papers, journal articles, conference publications, technical documentation, and official institutional websites. Relevant literature related to blockchain technology, academic certificate verification, MIT Blockcerts, and digital credential systems was reviewed and analyzed [3], [10]. Additional information was gathered from IEEE publications, blockchain research surveys, and educational technology reports [6], [8]. The collected data was organized and evaluated to identify key themes such as security, decentralization, verification efficiency, fraud prevention, and scalability. Secondary data collection enabled comprehensive understanding of existing blockchain-based educational credential systems without requiring primary experimental implementation.

Comparative Analysis Approach

The research uses a comparative analysis approach to evaluate differences between traditional certificate verification systems and blockchain-based digital credential systems. Parameters such as security, verification speed, transparency, data integrity, scalability, and fraud prevention capabilities were analyzed using information obtained from existing literature and case studies [5], [7]. The MIT Blockcerts framework was examined as a practical implementation example to assess real-world applicability and effectiveness [3], [10]. Comparative analysis also helped identify advantages and limitations associated with blockchain integration in educational institutions.

This approach supports objective evaluation of how blockchain technology improves academic certificate management and verification processes.

5.4 Tools and Technologies Used

This research primarily focuses on conceptual and analytical study rather than software development implementation. However, several blockchain-related technologies and tools discussed in the research include blockchain networks, cryptographic hashing algorithms, digital signature systems, and distributed ledger mechanisms [6]. The study also examines the Blockcerts framework developed by MIT for issuing and verifying blockchain-based academic credentials [10]. Additional technologies referenced include Bitcoin blockchain infrastructure, digital wallets, certificate verification platforms, and smart contract-based automation systems [11]. These technologies collectively support secure issuance, storage, sharing, and validation of academic certificates within blockchain-powered educational ecosystems.

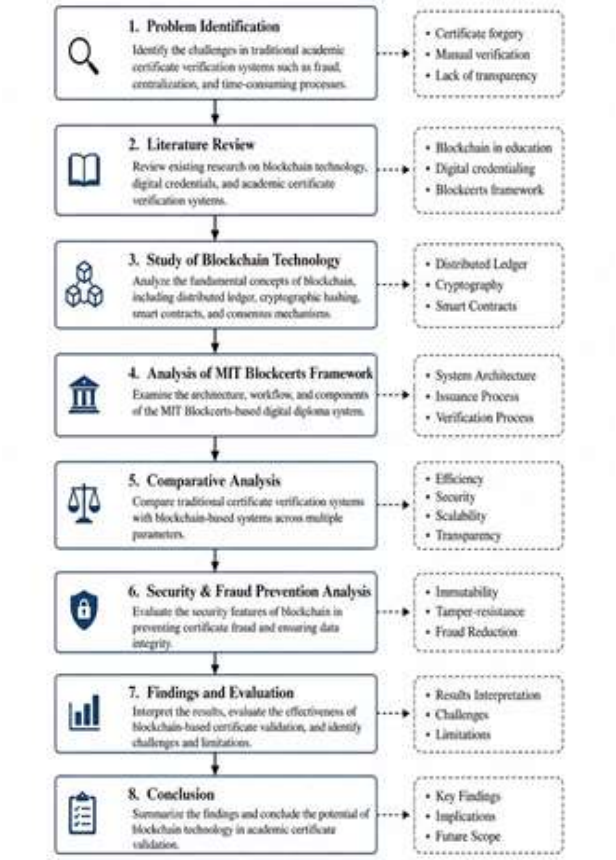

Fig. 3. Research Methodology Flowchart.

VI. ANALYSIS AND FINDINGS

Security Analysis

The analysis of blockchain-based academic certificate validation systems demonstrates significant improvements in security compared to traditional verification methods. Blockchain technology ensures data immutability through cryptographic hashing and decentralized storage mechanisms, making unauthorized modifications highly difficult [5], [6]. In the MIT Blockcerts framework, certificate data is digitally signed and anchored onto blockchain networks, providing secure proof of authenticity and integrity [3], [10]. Since blockchain records cannot be altered without consensus from participating nodes, the risk of certificate tampering and manipulation is substantially reduced. Furthermore, decentralized verification eliminates dependency on a single centralized database, thereby minimizing risks associated with system failures, unauthorized access, and data breaches [7]. The analysis indicates that blockchain technology offers a highly secure foundation for managing and validating academic credentials.

Fraud Prevention Capabilities

One of the major findings of this research is the effectiveness of blockchain technology in preventing academic certificate fraud. Traditional paper-based and centralized digital verification systems are vulnerable to forgery, duplication, and unauthorized modifications [8], [9]. Blockchain-based systems address these issues by creating immutable verification records linked through cryptographic hashing techniques [6]. In the Blockcerts framework, any alteration to a digital certificate changes its hash value, immediately invalidating verification results [10]. This mechanism prevents fake certificate generation and enables organizations to independently verify credential authenticity without relying entirely on institutional communication. The analysis shows that blockchain significantly improves trust and transparency within academic credential ecosystems while reducing opportunities for fraudulent activities.

Verification Efficiency

The study findings indicate that blockchain-based verification systems improve efficiency and reduce verification time compared to conventional methods. Traditional certificate validation often requires manual communication with educational institutions, resulting in delays and increased administrative workload [5]. Blockchain-powered systems such as MIT Blockcerts enable instant and automated verification processes through decentralized blockchain records [3]. Employers and institutions can independently verify certificates using digital signatures and blockchain proof without contacting the issuing authority directly [11]. This reduces operational costs, minimizes paperwork, and accelerates recruitment and admission procedures. The research concludes that blockchain technology enhances overall verification efficiency while simplifying credential management for students, universities, and employers.

Benefits of Blockchain-Based Validation

Blockchain-based academic certificate validation systems provide several important advantages over traditional verification approaches. The technology ensures secure and tamper-proof storage of academic credentials through distributed ledger mechanisms [4], [6]. Students gain ownership and portability of digital certificates, enabling secure sharing across institutions and employers [10].

Blockchain also improves transparency and trust by allowing independent credential verification without centralized dependency [7]. Additional benefits include reduced verification costs, faster processing, improved accessibility of records, and enhanced protection against certificate fraud [8]. The MIT Blockcerts implementation demonstrates how blockchain technology can modernize educational credential management systems while supporting efficient and reliable verification processes [3]. These findings highlight the transformative potential of blockchain in academic environments.

Challenges and Limitations

Despite its advantages, blockchain-based academic certificate validation systems face several technical and organizational challenges. One major limitation is scalability, as blockchain networks may experience performance issues and increased transaction costs when handling large volumes of data [4], [6]. Privacy concerns also arise because educational records contain sensitive personal information that must be protected from unauthorized exposure [5].

Integration of blockchain systems with existing institutional infrastructure can be complex and costly for universities with limited technical resources [7]. Additionally, lack of standardization and interoperability between blockchain platforms creates challenges for universal adoption of digital credential systems [8]. Legal, regulatory, and user adoption concerns further limit large-scale implementation of blockchain-based academic verification frameworks. These challenges indicate the need for further research and technological improvements.

VII. FUTURE SCOPE

Integration with Universities

Future development of blockchain-based academic credential systems may involve large-scale integration with universities and educational institutions worldwide. Educational organizations can adopt blockchain-powered verification frameworks to modernize certificate issuance, storage, and validation processes [7]. Integration with existing academic management systems could improve operational efficiency, reduce administrative workload, and enhance global accessibility of educational credentials. Wider institutional adoption may also contribute to establishing standardized and interoperable digital verification systems across different educational platforms [8]. As awareness and technical infrastructure improve, blockchain technology has the potential to become a core component of modern educational ecosystems.

Smart Contract Automation

Smart contracts offer significant future potential for automating academic certificate management and verification processes. Educational institutions may

use smart contracts to automatically issue digital certificates upon successful completion of academic requirements [6]. Verification procedures can also be automated, enabling employers and organizations to instantly validate credentials without manual intervention. Smart contract integration can improve transparency, reduce processing delays, and minimize administrative costs within educational institutions [8]. Future research may focus on developing more scalable and secure smart contract frameworks specifically designed for academic credential systems and decentralized educational platforms.

Global Academic Credential Networks

Blockchain technology has the potential to support the creation of global academic credential networks that enable secure and standardized verification of educational qualifications across countries and institutions. Such networks could facilitate international student mobility, employment verification, and global recognition of academic achievements [5], [7]. Blockchain-based credential ecosystems may allow universities, employers, and government agencies to securely exchange and validate educational records through decentralized platforms. Future advancements in interoperability and standardization could lead to globally connected academic verification systems that simplify credential sharing and improve trust in digital education records. This development could significantly transform international educational and employment verification processes.

VIII. CONCLUSION

This research paper examined the implementation of blockchain technology for academic certificate validation through a hybrid on-chain and off-chain blockchain architecture for academic certificate validation. The study analyzed the limitations of traditional certificate verification systems and explored how blockchain technology provides secure, decentralized, and tamper-resistant solutions for managing academic credentials. Existing literature and practical implementations demonstrate that blockchain-based systems improve transparency, verification efficiency, fraud prevention, and digital ownership of certificates [3], [10].

The research findings indicate that blockchain technology significantly enhances the security and reliability of academic credential verification through cryptographic hashing, distributed ledger mechanisms, and decentralized validation processes [5], [6]. The MIT Blockcerts framework demonstrates the practical feasibility of issuing and verifying blockchain-based digital diplomas while reducing dependence on manual institutional verification [11]. Furthermore, blockchain-powered systems simplify credential sharing and improve trust between educational institutions, students, and employers.

Despite these advantages, several challenges such as scalability, interoperability, privacy concerns, implementation complexity, and regulatory issues continue to affect large-scale adoption of blockchain-based academic verification systems [4], [8]. Therefore, further research and technological advancements are necessary to develop scalable, efficient, and universally accepted educational blockchain frameworks.

Overall, blockchain technology has strong potential to transform academic certificate management and verification systems by providing secure, transparent, and efficient digital credential solutions for future educational ecosystems.

Acknowledgment

The authors thank the anonymous reviewers whose critiques significantly strengthened this manuscript, and the GNIMS administration for providing the computational resources.

REFERENCES

1. MIT Open Learning, "The 'last mile' from credentials to employment," 2022. [Online]. Available: https://openlearning.mit.edu/news/last-mile-credentials-employment
2. MIT Registrar's Office, "Digital diplomas." [Online]. Available: http

s://registrar.mit.edu/transcripts-records/diplomas/digital-diplomas
3. Massachusetts Institute of Technology News, "Digital Diploma debuts at MIT," 2017. [Online]. Available: https:/ /news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017
4. A. et al., "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," 2023. [Online]. Available: http ://lnu.diva-portal.org/smash/record.jsf?pid=diva2%3A1775492
5. "Blockchain and Higher Education Diplomas," 2021. [Online]. Available: https: //pmc.ncbi.nlm.nih.gov/articles/PMC8314335/
6. "Digital Certificate Validation Using Blockchain: A Survey," IEEE Xplore. [Online]. Available: https ://ieeexplore.ieee.org/document/10226017/
7. "The Impact of the Blockchain on Academic Certificate Verification," 2021. [Online]. Available: https ://eudl.eu/doi/10.4108/eai.29-4-2021.169426
8. "A Blockchain-based Conceptual Model to Address Educational Certificate Verification," 2023. [Online]. Available: https: //www.etasr.com/index.php/ETASR/article/view/6170
9. "Certificate verification and validation using blockchain," 2019. [Online]. Available: ht tps://rjpn.org/jetnr/viewpaperforall.php?paper=JETNR2404 002
10. MIT Digital Credentials / Blockcerts materials. [Online].Available: https:/ /www.dci.mit.edu/posts/blockcerts-and-the-digital-certificates-project
11. MIT Media Lab, "Releases code for digital certificates on the blockchain," 2016. [Online]. Available: https ://bitcoinmagazine.com/business/mit-media-lab-releases-code-for-digital-certificates-on-the-blockchain-1465404945