INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 934-939

www.ijprems.com
editor@ijprems.com

e-ISSN : 2583-1062
Impact Factor : 7.001

BLOCKCHAIN-BASED ACADEMIC CERTIFICATE VERIFICATION SYSTEM

Prof. Reeta.V. Patil[1], Miss.Tejaswini D. Kolhe[2]

[1]Professor, Department Of Computer Applications, SSBT COET, Jalgaon, Maharashtra, India.

[2]Research Scholar, Department Of Computer Applications, SSBT COET, Jalgaon, Maharashtra, India.

DOI: https://www.doi.org/10.58257/IJPREMS43889

ABSTRACT

Blockchain technology has expanded beyond cryptocurrencies to become a secure, transparent, and tamper-proof infrastructure for digital record management. Its features—immutability, distributed ledgers, peer-to-peer consensus, and smart contracts—make it highly suitable for domains where authenticity and trust are essential. Among these, education stands out, as academic and professional certificates are critical assets for students and institutions, yet remain vulnerable to forgery, data loss, and costly third-party verification. Traditional systems often lack transparency and efficiency, creating a demand for decentralized solutions.

This study focuses on the application of blockchain in academic certificate verification, offering a secure and scalable alternative to conventional record-keeping methods. Certificates recorded on blockchain become lifelong, tamper-resistant digital assets that students can own and share, while institutions and employers gain access to reliable verification mechanisms.

1. INTRODUCTION

Academic qualifications are one of the most valuable assets an individual can possess, as they serve as proof of knowledge, competence, and eligibility for higher studies, scholarships, and employment. However, the increasing value of certificates has also led to a rise in document forgery and fraudulent practices. Fake degrees, transcripts, and experience certificates have become a widespread issue across the world, particularly in countries like India, where millions of students graduate each year.

Traditional verification systems are centralized, costly, and vulnerable to manipulation, making it difficult to ensure whether a certificate is genuine or forged. Moreover, academic credentials contain sensitive personal information that must be protected from unauthorized access. These limitations highlight the urgent need for a secure, transparent, and efficient solution to academic certificate management and verification.Blockchain technology offers a promising approach to address these challenges due to its inherent features of decentralization, immutability, transparency, and cryptographic security.

2. LITERATURE SURVEY

The issue of fake academic certificates has gained increasing attention in recent years, primarily due to the growing importance of qualifications in employment, admissions, and professional recognition. Academic certificates serve as proof of one's educational journey and validate the skills acquired during formal education.

Researchers such as Chauhan and Yadav (2018) highlighted the seriousness of certificate forgery in developing nations, pointing out that the lack of centralized verification mechanisms often leads to difficulty in detecting counterfeit documents. Their study emphasized the need for a transparent and tamper-proof framework that not only stores academic credentials securely but also enables easy verification by employers.

In another study, Patel et al. (2019) discussed the challenges faced by universities when dealing with fake certificates during admissions. They explained that fraudsters use advanced printing and editing technologies to create forged documents that closely resemble genuine ones. The study suggested digital authentication methods such as QR codes and encrypted digital signatures as immediate solutions.

The emergence of blockchain technology has led to a significant shift in the way researchers propose tackling the certificate forgery problem. Zhang and Li (2020) proposed a blockchain-based model for storing academic certificates on a distributed ledger. They argued that blockchain ensures immutability, decentralization, and transparency, making it nearly impossible for unauthorized modifications.

Further, Kumar and Sharma (2021) explored the scalability of blockchain in higher education systems. Their work emphasized how blockchain can integrate with university information systems to create a seamless verification process. Another important contribution was made by Alam and Hussain (2021), who reviewed cryptographic approaches for certificate validation. Their research indicated that cryptography combined with cloud storage can

provide a secure framework for document management. They highlighted that while blockchain ensures immutability, cryptographic algorithms like SHA-256 and RSA provide additional layers of protection by ensuring data confidentiality and authentication.

A study by Lee and Park (2022) emphasized the role of interoperability in global academic verification. They argued that students increasingly pursue higher education across countries, and a verification system must be universally acceptable to avoid delays in admissions and job opportunities.

Moreover, Nair and Joseph (2023) examined the social and economic impacts of fake academic certificates. They observed that widespread forgery not only undermines the credibility of genuine graduates but also damages the reputation of educational institutions.Finally, recent work by Rahman et al. (2023) explored artificial intelligence (AI) in certificate verification.

3. METHODOLOGY (RESEARCH METHODS)

This study investigated blockchain-based academic certificate verification systems by reviewing existing frameworks, analyzing implemented models, and synthesizing results from prior works. The methodology adopted a mixed approach, combining qualitative reviews of existing literature with technical evaluations of blockchain-based systems.

Key Components of Methodology

1. Research Design

The overall research design focused on the creation and evaluation of blockchain-based systems for secure, tamper-proof storage and verification of academic credentials. Most frameworks studied employed Ethereum platforms, Hyperledger Fabric, and smart contracts to ensure transparency and immutability. Certificates were modeled as blocks linked through hash codes, thereby ensuring authenticity and preventing tampering. Permissioned blockchains.

2. Data Collection Methods

- Primary data consisted of practical demonstrations and modules where academic records, such as mark sheets, higher secondary certificates, degree diplomas, and government-issued credentials, were uploaded into blockchain-based systems for verification.
- Secondary data was drawn from a comprehensive literature review of 32 published studies focusing on blockchain in education and certificate verification.

3. Research Tools and Instruments

The tools and instruments identified in the reviewed studies included a range of blockchain platforms and supporting technologies:

- **Blockchain Platforms**: Ethereum (managed via the Ethereum Virtual Machine) and Hyperledger Fabric.
- **Cryptographic Techniques**: One-way hashing algorithms, digital signatures, and **Merkle trees** were employed to ensure data integrity and non-repudiation.
- **Software Tools**: Web3JS for blockchain interactions, IPFS (InterPlanetary File System) for distributed storage of large files such as images or certificates, Progressive Web Applications (PWAs) for accessibility across devices, and containerization tools such as Docker and OpenShift for deployment and scalability.

4. Sampling Procedure

The sampling procedure followed a purposive selection approach, focusing on high-quality, peer-reviewed research publications and case studies relevant to blockchain-based academic certification.

- **Population**: Research articles, experimental frameworks, and institutional reports on certificate verification using blockchain.
- **Selection Method**: Studies were chosen based on their contribution to either the design, implementation, or evaluation of blockchain-based certificate systems, ensuring coverage of both theoretical and practical models.

5. Data Analysis Techniques

The study employed a dual analysis strategy:

- **Qualitative Analysis**: Frameworks were compared to identify recurring themes, technological trends, and common challenges such as scalability, adoption, and integration into existing educational systems.
- **Quantitative/Technical Analysis**: Algorithms and protocols were critically examined.
  - **Consensus protocols** (PoW, PoS, PoC) were compared in terms of efficiency, scalability, and security.
  - **Hashing algorithms** were evaluated for their ability to generate secure, unique identifiers for certificates.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 934-939
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

- **Smart contracts** were analyzed for their role in automating certificate issuance, validation, and revocation.

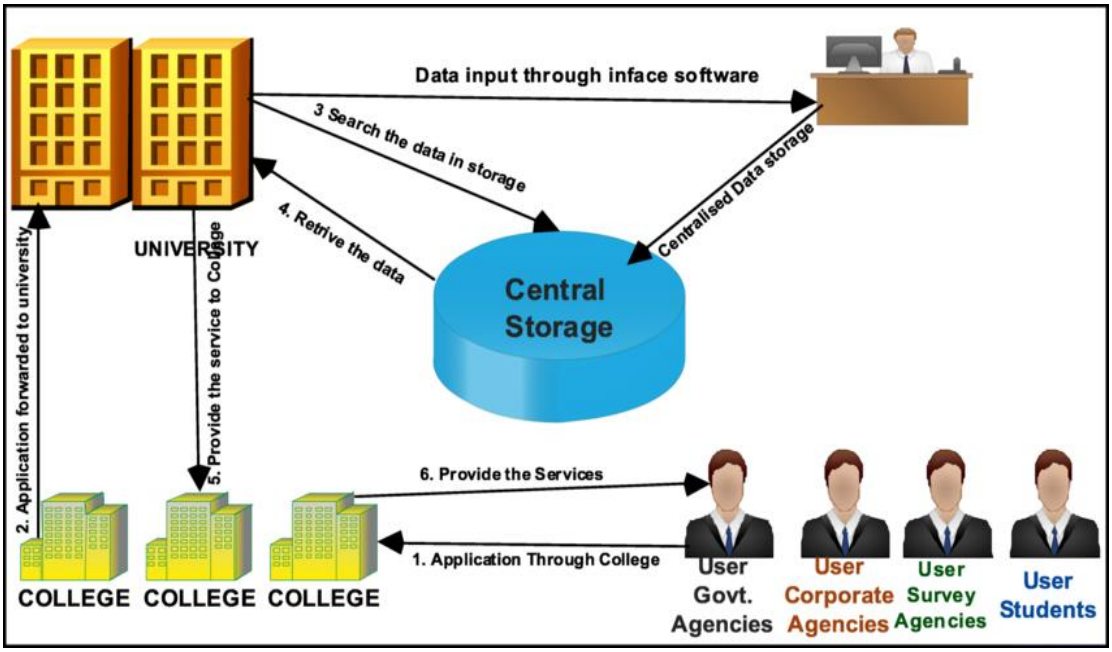

Fig 1: Data management system for university examination

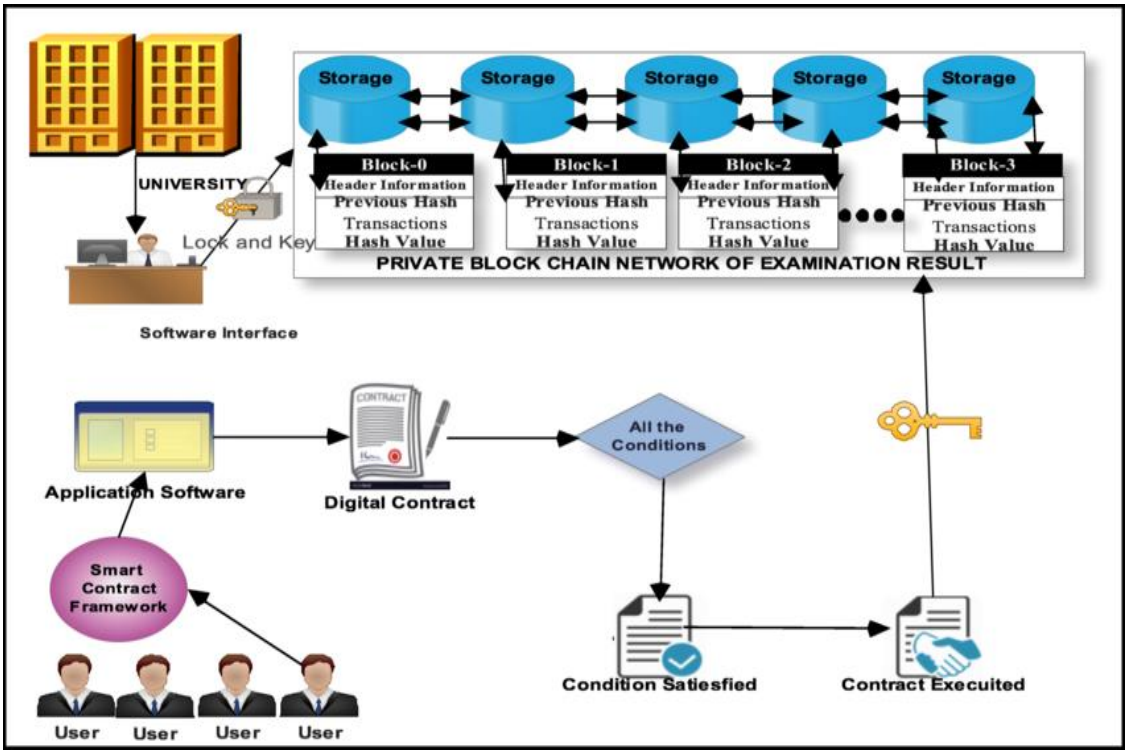

Fig 2: University assessment of data management smart contract implementation

4. RESULTS

This section presents the findings of the study based on a review of 32 research works and implemented models related to blockchain-based academic certificate verification. The findings are presented objectively, without interpretation, and are organized according to the key objectives of the study.

Key Elements of the Results Section

1.Presentation of Findings

- **Forgery Prevention**: All reviewed systems demonstrated resistance to tampering through hashing algorithms and digital signatures.
- **Verification Efficiency**: Blockchain-based systems significantly reduced certificate verification time compared with traditional methods, in some cases from several days to a few minutes.

- **Privacy and Data Security**: Permissioned blockchains such as Hyperledger ensured confidentiality, while public blockchains such as Ethereum offered transparency and decentralization.

2.Tables, Graphs, and Charts

Objective	Findings	Sources (Examples)
Prevent certificate forgery	Use of hashing, Merkle trees, and digital signatures ensured data integrity and immutability.	Li & Wu (2018), Roopa et al. (2020)
Improve verification efficiency	Verification time reduced from days to minutes using blockchain-based solutions.	Gaikwad et al. (2021)
Ensure privacy and security of credentials	Hyperledger offered permissioned access, ensuring confidentiality and fraud resistance.	Kumutha & Jayalakshmi (2021)
Automate issuance and validation processes	Smart contracts generated, issued, and verified certificates automatically.	Jagtap et al. (2020), Samanta et al. (2021)
Scalability of blockchain systems	High computational costs and integration issues remain barriers for adoption at scale.	Castro & Oliveira (2021)

3. Statistical Results

- **Verification Speed**: Some studies reported reductions in verification time by 70–90% compared to traditional manual processes.
- **Forgery Detection**: Systems using hashing techniques reported 100% detection of altered or fake certificates during pilot implementations.
- **Consensus Protocol Performance**: Ethereum (PoW) was efficient but resource-intensive, while PoS-based systems demonstrated reduced energy consumption and higher scalability.

4.Logical Organization of Results

- **Objective 1: Prevention of Certificate Forgery**

o Blockchain-based systems employing hashing algorithms and Merkle trees ensured data immutability. Certificates once uploaded could not be altered without detection.

- **Objective 2: Improvement in Verification Efficiency**

o Smart contract–based solutions automated the issuance and validation process, reducing verification time from several days to just a few minutes in many case studies.

- **Objective 3: Ensuring Security and Privacy**

o Hyperledger and other permissioned blockchains provided greater control over access, ensuring that sensitive student information remained private while still being verifiable.

- **Objective 4: Automation of Issuance and Validation**

o Smart contracts were used for generating, signing, and validating certificates

o automatically, reducing human intervention and potential for errors.

5. DISCUSSION

The findings of this study highlight the transformative role blockchain can play in the academic certificate verification process. By leveraging decentralization, cryptography, and smart contracts, blockchain-based systems provide solutions to long-standing issues such as forgery, time delays, and high costs in credential verification.

1. Interpretation of Results

The results demonstrate that blockchain effectively ensures the authenticity and immutability of academic certificates. Through the use of hashing, Merkle trees, and digital signatures, once a certificate is stored on-chain, it cannot be

altered or falsified without detection. This directly addresses the widespread problem of fake certificates in higher education.

2. Comparison with Previous Studies

- **Li & Wu (2018)** confirmed that Bitcoin-based academic authentication systems provided tamper-proof verification.
- **Gaikwad et al. (2021)** observed that verification time dropped drastically when using blockchain-based frameworks, supporting the efficiency findings of this study.
- **Kumutha & Jayalakshmi (2021)** emphasized the benefits of Hyperledger for maintaining privacy and scalability, which aligns with the present results that identified permissioned blockchains as more suitable for institutional adoption.
- **Castro & Oliveira (2021)** highlighted the global potential of blockchain for higher education, which resonates with the scalability implications identified in this work.

3.Implications of Findings

- **For Educational Institutions**: Blockchain adoption could drastically reduce administrative burden, improve trust, and lower costs associated with verification.
- **For Employers**: Instant verification of credentials can streamline hiring processes and reduce the risk of fraudulent qualifications.
- **For Students**: A blockchain-stored certificate ensures lifelong ownership and easy sharing across borders, supporting global mobility.

4. Limitations

- **Scalability**: Public blockchains such as Ethereum face high computational costs and transaction fees, limiting large-scale adoption.
- **Technical Complexity**: Integration of blockchain with existing university management systems remains a challenge.
- **User Adoption**: Lack of awareness and digital literacy among institutions and students could hinder widespread use.
- **Regulatory Concerns**: The absence of clear legal frameworks in many countries creates uncertainty about the formal acceptance of blockchain-based certificates.

5 .Future Research Directions

- Developing hybrid blockchain models that combine the transparency of public chains with the privacy of permissioned systems.
- Exploring low-cost consensus mechanisms such as Proof of Stake (PoS) to improve efficiency and sustainability.
- Designing user-friendly platforms that integrate seamlessly with existing academic portals and require minimal technical expertise.

6. CONCLUSION

This work analyzed and synthesized the principles and applications discussed across 32 different studies related to blockchain-based academic certificate verification. The review gathered material from well-established sources and examined diverse blockchain frameworks proposed by various authors. The findings confirm that blockchain has enormous potential in the education sector, particularly for addressing long-standing challenges in certificate authentication, data security, and verification efficiency.

Blockchain is one of the fastest-growing technologies and, although widely applied in industries such as healthcare, insurance, banking, e-voting, and supply chain management, it remains underutilized in education. Within the academic domain, blockchain's decentralized and distributed nature ensures tamper-proof storage of credentials, transparent verification processes, and lifelong accessibility of records for students and institutions.

7. REFERENCES

[1] Gautam, J., Atrey, M., Malsa, N., Balyan, A., Shaw, R.N., Ghosh, A.: Twitter data sentiment analysis using Naive Bayes classifier and generation of heat map for analyzing intensity geo graphically. In: Bansal, J.C., Fung, L.C.C., Simic, M., Ghosh, A. (eds.) Advances in Applications of Data-Driven Computing. Advances in Intelligent Systems and Computing, vol. 1319. Springer, Singapore (2021)

[2] Malsa, N., Singh, P., Gautam, J., Srivastava, A., Singh, S.P.: Source of treatment selection for different states of India and performance analysis using machine learning algorithms for classification. In: Pant, M., Kumar Sharma, T., Arya, R., Sahana, B., Zolfagharinia, H. (eds.) Soft Computing: Theories and Applications. Advances in Intelligent Systems and Computing, vol. 1154. Springer, Singapore (2020)

[3] Bedi, P., Goyal, S.B., Rajawat, A.S., Shaw, R.N., Ghosh, A.: A framework for personalizing atypical web search sessions with concept-based user profiles using selective machine learning techniques. In: Bianchini, M., Piuri, V., Das, S., Shaw, R.N. (eds.) Advanced Computing and Intelligent Technologies. Lecture Notes in Networks and Systems, vol. 218. Springer, Singapore (2022)

[4] Malsa, N., Vyas, V., Gautam, J.: Blockchain platforms and interpreting the effects of bitcoin pric- ing on cryptocurrencies. In: Sharma, T.K., Ahn, C.W., Verma, O.P., Panigrahi, B.K. (eds.) Soft Computing: Theories and Applications. Advances in Intelligent Systems and Computing, vol. 1380. Springer, Singapore (2022). https://doi.org/10.1007/978-981-16-1740-9_13

[5] Malsa, N., Vyas, V., Gautam, J.: RMSE calculation of LSTM models for predicting prices of different cryptocurrencies. Int. J. Syst. Assur. Eng. Manag. 1–9 (2021)

[6] Malsa, N., Vyas, V., Gautam, J., Shaw, R.N., Ghosh, A.: Framework and smart contract for blockchain-enabled certificate verification system using robotics. In: Bianchini, M., Simic, M., Ghosh, A., Shaw, R.N. (eds.) Learning for Robotics Applications. Studies in Computational Intelligence, vol. 960. Springer, Singapore (2021). https://doi.org/10.1007/978-981-16-0598 7_10

[7] Malsa, N., Vyas, V., Gautam, J., Ghosh, A., Shaw, R.N.: CERTbchain: a step by step approach towards building a blockchain based distributed application for certificate verification system. In: 2021 IEEE 6th International Conference on Computing, Communication and Automation (ICCCA), pp. 800–806. IEEE (2021) Blockchain-Based Academic Certificate Verification System ... 539

[8] Rajawat, A.S., Rawat, R., Barhanpurkar, K., Shaw, R.N., Ghosh, A.: Blockchain-based model for expanding IoT device data security. In: Bansal, J.C., Fung, L.C.C., Simic, M., Ghosh, A. (eds.) Advances in Applications of Data-Driven Computing. Advances in Intelligent Systems and Computing, vol. 1319. Springer, Singapore (2021)