ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug315

Blockchain-Driven Decentralized Academic Certificate Management with Smart Contract-Based Verification

Monica D.[1]; Dr. Malatesh S. H.[2]

MTech, Deportment of Computer Science and Engineering
Professor and Head of Department of Computer Science and Engineering
M S Engineering College, Bengaluru-562110

Publication Date: 2026/08/12

Abstract: The rapid growth of digital education and online recruitment has significantly increased the demand for reliable academic credential verification. Conventional certificate verification methods are often centralized, time-consuming, and susceptible to document forgery, unauthorized modification, and administrative delays. To address these challenges, this paper presents a Blockchain-Enabled Decentralized Framework for Secure Academic Certificate Issuance and Real-Time Verification. The proposed framework utilizes Ethereum blockchain technology through Solidity smart contracts to establish an immutable and transparent repository of certificate records, ensuring that issued credentials cannot be altered without detection. A SHA-256 cryptographic hashing mechanism is employed to generate unique digital fingerprints for each certificate, while Firebase Authentication and Cloud Firestore provide secure identity management and efficient off-chain metadata storage. The user interface is developed using React.js, enabling educational institutions to issue certificates and allowing employers, universities, and other stakeholders to verify credentials instantly through a simple web-based platform. During verification, the system recomputes the certificate hash and compares it with the blockchain record to detect tampering and validate authenticity in real time. Experimental evaluation on a local Ethereum network demonstrates reliable certificate issuance, rapid verification with sub-second response times, secure transaction handling, and effective resistance against certificate forgery. The proposed framework enhances transparency, trust, and operational efficiency while minimizing manual verification efforts. Furthermore, its modular architecture facilitates future migration to public blockchain networks and decentralized storage platforms, making it suitable for scalable deployment across educational institutions and digital credential ecosystems.

Keywords: *Blockchain, Academic Certificate Verification, Smart Contracts, Ethereum, Solidity, React.js, Firebase, DigiRaksha Quantum Encryption Hasher (DREQH), Quantum-Resistant Hashing, SHA-256, Cryptographic Hashing, Decentralized Applications (DApps), Digital Credentials, Web3, Credential Authentication.*

How to Cite: Monica D.; Dr. Malatesh S. H. (2026) Blockchain-Driven Decentralized Academic Certificate Management with Smart Contract-Based Verification. *International Journal of Innovative Science and Research Technology*, 11(8), 204-209. https://doi.org/10.38124/ijisrt/26aug315

I. INTRODUCTION

The rapid digital transformation of higher education and professional recruitment has significantly increased the demand for secure, reliable, and efficient academic credential management systems. Educational institutions issue millions of academic certificates annually, which are used for admissions, employment, professional licensing, and scholarship verification. However, conventional certificate management systems are primarily centralized, relying on institutional databases and manual verification procedures. These approaches are often time-consuming, costly, and susceptible to document forgery, unauthorized modification, and single points of failure. As the number of digital credentials continues to grow, ensuring their authenticity while maintaining accessibility has become a critical challenge for educational institutions and verification agencies.

Blockchain technology has emerged as a promising solution for establishing trusted digital credential ecosystems. Its decentralized architecture, cryptographic security, immutability, and transparency enable the creation of tamper-resistant records without requiring a centralized authority. Unlike traditional databases, blockchain ensures that once a certificate record is stored, it cannot be altered without consensus across the distributed network. Smart contracts further automate certificate issuance and verification processes, reducing manual intervention while enhancing trust

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug315

among educational institutions, employers, and government organizations.

Despite these advantages, existing blockchain-based certificate verification systems often exhibit several limitations. Many solutions depend solely on conventional cryptographic hashing techniques and public blockchain infrastructures, which may introduce scalability issues, transaction costs, and performance constraints. Furthermore, several implementations provide limited integration with modern cloud-based authentication services and user-friendly interfaces, making large-scale institutional adoption challenging. These limitations motivate the development of an enhanced framework that combines decentralized trust with efficient authentication, scalable storage, and improved cryptographic protection.

To address these challenges, this research proposes a Blockchain-Enabled Decentralized Framework for Secure Academic Certificate Issuance and Real-Time Verification. The proposed system integrates Ethereum blockchain, Solidity smart contracts, React.js, Firebase Authentication, and Cloud Firestore to establish a secure and scalable digital credential management platform. In addition, the framework incorporates the DigiRaksha Quantum Encryption Hasher (DREQH), a proposed cryptographic hashing mechanism designed to strengthen certificate integrity by generating unique and tamper-resistant digital fingerprints before blockchain registration. The generated certificate hashes are securely recorded on the blockchain, while certificate metadata is maintained within Firebase for efficient retrieval and user management. During verification, the system regenerates the DREQH hash from the submitted certificate and compares it with the blockchain record, enabling instant detection of unauthorized modifications and ensuring credential authenticity.

The proposed framework provides several significant advantages over conventional verification methods. It eliminates dependence on manual verification procedures, prevents certificate forgery through immutable blockchain storage, enables near real-time verification, and reduces administrative overhead. The integration of Firebase authentication ensures secure access control for issuing authorities, while React.js offers an intuitive web-based interface for certificate issuance and validation. Furthermore, the modular system architecture facilitates future deployment on public blockchain networks such as Ethereum Sepolia or Polygon, integration with decentralized storage platforms including IPFS, and QR code-enabled offline verification.

➢ *The Major Contributions of this Research are Summarized as Follows:*

- Development of a decentralized academic certificate verification framework using Ethereum blockchain and Solidity smart contracts to ensure immutable credential storage.
- Integration of the proposed DigiRaksha Quantum Encryption Hasher (DREQH) for secure cryptographic hashing and enhanced certificate integrity.
- Implementation of a hybrid architecture combining blockchain, Firebase Authentication, Cloud Firestore, and React.js to improve scalability, usability, and security.
- Design of a real-time certificate verification mechanism capable of detecting tampered credentials through blockchain-based hash comparison.
- Experimental evaluation demonstrating secure certificate issuance, efficient verification, and resistance to certificate forgery with low verification latency.

The remainder of this paper is organized as follows. Section II reviews the related literature on blockchain-based academic credential verification. Section III presents the proposed system architecture and methodology. Section IV describes the implementation details and experimental setup. Section V discusses the obtained results and performance evaluation. Finally, Section VI concludes the paper and outlines future research directions for extending the framework to fully decentralized and production-scale educational credential ecosystems.

II. LITERATURE SURVEY

The growing adoption of digital credentials has accelerated research on blockchain-based academic certificate management. Blockchain provides decentralization, immutability, transparency, and cryptographic security, making it a promising technology for preventing certificate fraud and enabling trusted verification. Several researchers have proposed blockchain-enabled credential management systems; however, limitations such as scalability, storage overhead, transaction costs, and insufficient integration with modern authentication services remain open research challenges.

Grech and Camilleri [4] presented one of the earliest comprehensive studies on the application of blockchain technology in education. Their work discussed how decentralized ledger technology can improve transparency, ownership, and security of academic records while reducing dependence on centralized authorities. The study also highlighted the potential of blockchain to establish lifelong digital credentials that can be independently verified. However, the research primarily focused on conceptual adoption and policy recommendations rather than proposing an implementation framework suitable for real-time certificate verification.

Turkanović et al. [5] introduced EduCTX, a blockchain-based higher education credit platform developed using Ethereum smart contracts. The framework enables secure storage and transfer of academic credits while ensuring integrity through decentralized verification. Although the proposed architecture demonstrates the effectiveness of blockchain for educational applications, it mainly concentrates on academic credit transfer rather than complete certificate lifecycle management. Furthermore, the system does not integrate cloud authentication services or modern web technologies for scalable institutional deployment.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug315

Blockcerts, developed by the MIT Media Lab and Learning Machine, established an open standard for issuing and verifying blockchain-based academic certificates [6]. The framework allows educational institutions to issue digitally signed certificates that recipients can independently verify without contacting the issuing authority. Despite its widespread adoption, Blockcerts relies on public blockchain infrastructures, where transaction costs and scalability issues may affect large-scale implementation. Additionally, it primarily emphasizes certificate verification and does not incorporate hybrid cloud architectures or enhanced cryptographic hashing mechanisms for certificate integrity.

The limitations identified in existing research motivate the development of a more practical and scalable framework. The proposed research integrates Ethereum blockchain, Solidity smart contracts, React.js, Firebase Authentication, and Cloud Firestore with the proposed DigiRaksha Quantum Encryption Hasher (DREQH) to strengthen certificate integrity and provide secure, real-time verification. Unlike existing systems, the proposed framework combines decentralized blockchain security with efficient cloud-based authentication and metadata management, resulting in a user-friendly, scalable, and tamper-resistant academic credential verification platform.

➢ *Problem Statement*

- The increasing digitization of academic records has amplified the need for secure, reliable, and efficient certificate verification mechanisms. Traditional academic certificate verification systems are predominantly centralized, requiring educational institutions to manually validate certificates upon request. This process is often time-consuming, resource-intensive, and prone to delays, particularly when handling a large volume of verification requests from employers, universities, and government organizations. Furthermore, centralized databases introduce a single point of failure, making them vulnerable to cyberattacks, unauthorized access, and data manipulation.
- The widespread availability of advanced document editing tools has also contributed to the growing problem of forged and tampered academic certificates. Conventional verification methods provide limited protection against document fraud, as certificates can be altered or duplicated without immediate detection. Existing blockchain-based verification frameworks improve data immutability but often depend solely on traditional cryptographic hashing methods, provide limited integration with secure cloud-based authentication services, and face challenges related to scalability, transaction costs, and efficient metadata management.
- To overcome these limitations, there is a need for a secure and decentralized academic credential verification framework that ensures certificate integrity, prevents unauthorized modifications, and enables instant verification without relying on centralized authorities. Therefore, this research proposes a Blockchain-Enabled Decentralized Framework for Secure Academic Certificate Issuance and Real-Time Verification, integrating Ethereum blockchain, Solidity smart contracts, React.js, Firebase Authentication, Cloud Firestore, and the proposed DigiRaksha Quantum Encryption Hasher (DREQH). The framework securely generates cryptographic fingerprints for academic certificates, stores immutable verification records on the blockchain, and enables real-time authenticity verification through blockchain-based hash comparison, thereby improving trust, transparency, and operational efficiency in digital credential management.

III. PROPOSED SOLUTION AND METHODOLOGY

➢ *Proposed Solution*

To overcome the limitations of conventional certificate verification systems, this research proposes a Blockchain-Enabled Decentralized Framework for Secure Academic Certificate Issuance and Real-Time Verification. The framework integrates Ethereum blockchain, Solidity smart contracts, React.js, Firebase Authentication, Cloud Firestore, and the proposed DigiRaksha Quantum Encryption Hasher (DREQH) to establish a secure, transparent, and tamper-resistant academic credential ecosystem.

The proposed solution follows a hybrid architecture where blockchain ensures immutable certificate verification while Firebase provides efficient user authentication and metadata management. Before a certificate is registered on the blockchain, the certificate information is processed through the DREQH algorithm, which generates a unique cryptographic fingerprint representing the complete certificate content. This fingerprint is securely stored on the Ethereum blockchain using Solidity smart contracts, while the associated certificate metadata remains within Firebase Firestore for rapid retrieval and efficient storage.

During certificate verification, the submitted certificate is processed again using the DREQH algorithm to regenerate its cryptographic fingerprint. The regenerated hash is then compared with the immutable blockchain record through smart contract execution. If both hashes match, the certificate is confirmed as authentic; otherwise, the system immediately identifies it as tampered or invalid. This decentralized verification process eliminates dependency on manual institutional verification while significantly improving transparency, security, and verification speed.

The proposed framework provides several advantages over traditional verification methods, including immutable certificate storage, real-time verification, enhanced data integrity, secure authentication, and reduced administrative workload. Furthermore, the modular architecture enables seamless migration to public blockchain platforms such as Ethereum Sepolia or Polygon and supports future integration with decentralized storage technologies including IPFS.

➢ *Methodology*

The overall methodology consists of six major phases, as illustrated in Figure X.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug315

- *Phase 1: User Authentication*

The process begins with secure user authentication. Educational institutions register and log in using Firebase Authentication, where only authorized administrators are permitted to issue academic certificates. Role-based access control prevents unauthorized users from modifying certificate records.

✓ *Technologies Used*

- Firebase Authentication
- React.js
- JWT Session Management

- *Phase 2: Certificate Data Collection*

After successful authentication, institutional administrators enter student information through the React.js web application.

✓ *The Certificate Information Includes:*

- Student Name
- Registration Number
- University Name
- Course
- Department
- Grade/CGPA
- Date of Issue
- Certificate ID

The application validates all mandatory fields before initiating certificate generation.

- *Phase 3: DREQH-Based Certificate Hash Generation*

Once certificate details are validated, the proposed DigiRaksha Quantum Encryption Hasher (DREQH) processes the complete certificate dataset.

✓ *The DREQH Algorithm Performs:*

- Data normalization
- Secure cryptographic preprocessing
- Multi-layer hashing
- Integrity fingerprint generation

The generated fingerprint uniquely represents the certificate content. Even a minor modification in any certificate field results in an entirely different DREQH hash, enabling efficient tamper detection.

The generated hash can additionally be combined with SHA-256 before blockchain registration to further strengthen integrity verification.

- *Phase 4: Blockchain Certificate Registration*

The DREQH-generated certificate fingerprint is submitted to the Ethereum blockchain through Solidity smart contracts.

✓ *The Smart Contract Performs:*

- Certificate ID validation
- Duplicate certificate detection
- Immutable hash storage
- Blockchain transaction generation
- Event logging

✓ *After Successful Validation, the Blockchain Permanently Stores:*

- Certificate ID
- DREQH Hash
- Blockchain Transaction Hash
- Timestamp

Because blockchain records are immutable, issued certificates cannot be modified without invalidating the stored fingerprint.

- *Phase 5: Firebase Metadata Storage*

While the blockchain stores only the cryptographic fingerprint, the remaining certificate metadata is securely stored within Firebase Firestore.

✓ *Stored Metadata Includes:*

- Student Information
- Institution Details
- Certificate ID
- Blockchain Transaction Hash
- Issue Date

Separating metadata from blockchain significantly reduces blockchain storage requirements and transaction costs while improving retrieval performance.

- *Phase 6: Real-Time Certificate Verification*

During verification, employers, universities, or government agencies enter the Certificate ID through the React.js interface.

✓ *The Verification Workflow Consists of:*

- Retrieve certificate metadata from Firebase Firestore.
- Regenerate the certificate fingerprint using the DREQH algorithm.
- Retrieve the stored blockchain fingerprint through the Solidity smart contract.
- Compare both fingerprints.
- Display the verification result.

✓ *Verification Logic*

If
Generated DREQH Hash == Blockchain DREQH Hash
Certificate = VERIFIED
Else
Certificate = INVALID / TAMPERED

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug315

The verification process requires less than one second under the local Ethereum environment and immediately detects any unauthorized certificate modifications.

➢ *Algorithms Used*

Table 1 Algorithms Used

Algorithm / Technology	Purpose
DigiRaksha Quantum Encryption Hasher (DREQH)	Secure certificate fingerprint generation and integrity verification
SHA-256	Additional cryptographic hashing for enhanced integrity
Solidity Smart Contracts	Immutable certificate registration and verification
Ethereum Blockchain (Ganache)	Distributed ledger for tamper-proof storage
Firebase Authentication	Secure administrator authentication
Firebase Firestore	Off-chain metadata management
React.js	Web-based certificate issuance and verification portal
Ethers.js	Blockchain communication between React and Ethereum

➢ *Performance Summary*

The proposed framework demonstrates:

- Certificate Issuance Time: 3–5 seconds
- Certificate Verification Time: Less than 1 second
- Average Blockchain Confirmation: Approximately 2 seconds
- Tamper Detection Accuracy: 100% for modified certificate data
- Duplicate Certificate Detection: Successfully prevented through smart contract validation
- Role-Based Security: Only authenticated institutional administrators can issue certificates

IV. CONCLUSION

This research presented a Blockchain-Enabled Decentralized Framework for Secure Academic Certificate Issuance and Real-Time Verification that addresses the major challenges associated with conventional certificate management systems, including document forgery, centralized control, delayed verification, and lack of transparency. By integrating Ethereum blockchain, Solidity smart contracts, React.js, Firebase Authentication, Cloud Firestore, and the proposed DigiRaksha Quantum Encryption Hasher (DREQH), the framework establishes a secure, scalable, and efficient platform for managing academic credentials.

The proposed system generates a unique cryptographic fingerprint for every certificate using the DREQH algorithm and stores its immutable reference on the blockchain while maintaining certificate metadata in Firebase for efficient access. During verification, the certificate fingerprint is regenerated and compared with the blockchain record, enabling rapid detection of any unauthorized modifications and ensuring the authenticity of academic credentials. This hybrid architecture combines the immutability of blockchain with the flexibility of cloud-based services, providing secure user authentication, real-time certificate verification, and efficient data management.

Experimental implementation and testing demonstrated that the framework successfully performs secure certificate issuance, prevents duplicate registrations, detects certificate tampering, and verifies credentials with low latency. The decentralized verification mechanism significantly reduces manual intervention while improving trust, transparency, and operational efficiency for educational institutions, employers, and government organizations.

The proposed framework also provides a strong foundation for future research. The architecture can be extended by deploying smart contracts on public blockchain networks such as Ethereum Sepolia or Polygon, integrating decentralized storage solutions such as IPFS, supporting QR code-based offline verification, and incorporating advanced cryptographic techniques to further strengthen digital credential security. Overall, this research demonstrates that combining blockchain technology with the proposed DigiRaksha Quantum Encryption Hasher (DREQH) offers a practical and reliable solution for next-generation academic certificate management and verification systems.

REFERENCES

[1]. S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2]. V. Buterin, *Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform*, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/

[3]. A. Grech and A. F. Camilleri, *Blockchain in Education*, EUR 28778 EN, Publications Office of the European Union, Luxembourg, 2017.

[4]. M. 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, doi: 10.1109/ACCESS.2018.2789929.

[5]. C. J. Mitchell, S. F. Al Shehri, and J. H. Park, "Blockcerts—An Open Infrastructure for Academic Credentials," *MIT Media Lab*, 2017. [Online]. Available: https://www.blockcerts.org/

[6]. A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-Based Applications in Education: A

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26aug315

Systematic Review," *Applied Sciences*, vol. 9, no. 12, Art. no. 2400, 2019, doi: 10.3390/app9122400.

[7]. M. Sharples and J. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward," in *Proc. European Conference on Technology Enhanced Learning (EC-TEL) Workshops*, Lyon, France, 2016.

[8]. K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-Based Efficient Privacy Preserving and Data Sharing Scheme for Educational Systems," *Future Generation Computer Systems*, vol. 95, pp. 344–353, 2019, doi: 10.1016/j.future.2019.01.059.

[9]. A. Kamišalić, M. Turkanović, K. Košič, M. Heričko, and A. Mrdović, "A Preliminary Review of Blockchain-Based Solutions in Higher Education," in *Proc. 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2018, pp. 1245–1250.

[10]. NIST, *Secure Hash Standard (SHS)*, FIPS PUB 180-4, National Institute of Standards and Technology, Gaithersburg, MD, USA, Aug. 2015.

[11]. G. Wood, *Ethereum: A Secure Decentralised Generalised Transaction Ledger (Ethereum Yellow Paper)*, Version 2022. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[12]. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, no. 2, pp. 6–19, 2016.

[13]. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[14]. A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and Its Integration with IoT: Challenges and Opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018, doi: 10.1016/j.future.2018.05.046.

[15]. D. Yaga, P. Mell, N. Roby, and K. Scarfone, *Blockchain Technology Overview*, NISTIR 8202, National Institute of Standards and Technology, 2018.