B-LOCK: A Blockchain-Based Certificate Validation System for Secure Academic Document Verification

Dr. Kanigiri Suresh[1], Kasireddy Rammohan Reddy[2], CH Manohar[3], Allanki Shivani[4], Dharavath Pushpa Geeetha[5]

[1]Asst Professor, Department of CSE-AIML, AVN Institute Of Engineering & Technology, Rangareddy, Telangana
Email: kanigirisuresh@gmail.com

[2]B.Tech, Department of CSE-AIML, AVN Institute Of Engineering & Technology, Rangareddy, Telangana
Email: rammohanreddy774@gmail.com

[3]B.Tech, Department of CSE-AIML, AVN Institute Of Engineering & Technology, Rangareddy, Telangana
Email: manoharmsr2030@gmail.com

[4]B.Tech, Department of CSE-AIML, AVN Institute Of Engineering & Technology, Rangareddy, Telangana
Email: shivani8307@gmail.com

[5]B.Tech, Department of CSE-AIML, AVN Institute Of Engineering & Technology, Rangareddy, Telangana
Email: dharavathgeetha@gmail.com

ABSTRACT

The rapid adoption of digital academic certificates has simplified document sharing but has also increased the risk of forgery and unauthorized alterations. Existing verification approaches are often dependent on manual validation or centralized databases, which are time-consuming and vulnerable to manipulation. This paper presents **B-LOCK**, a blockchain-driven system designed to provide a secure and efficient method for certificate authentication. In the proposed system, each certificate is processed to generate a unique SHA-256 hash that acts as its digital identity. This hash is stored on a blockchain network using a Proof-of-Work consensus mechanism, ensuring immutability and transparency. During verification, the uploaded document is rehashed and compared with the stored value to confirm authenticity. Any discrepancy immediately indicates tampering. Additionally, the system prevents duplicate certificate submissions and supports role-based access for validation authorities. Experimental evaluation shows that the system performs reliably with consistent verification speed. The B-LOCK model demonstrates how blockchain and cryptographic techniques can be effectively combined to build a trustworthy academic verification framework.

Key Words: Blockchain, Certificate Verification, SHA-256 Hashing, Proof-of-Work, Document Security, Academic Credentials, Document Integrity.

1.INTRODUCTION

Academic certificates serve as formal proof of an individual's educational qualifications and are widely used by employers, academic institutions, and organizations for decision-making purposes. These documents play a critical role in evaluating a candidate's eligibility for employment, higher education, and professional opportunities. With the rapid shift toward digitalization, academic records are increasingly stored, shared, and verified in electronic formats, improving accessibility and convenience. Despite these advantages, the digital transformation of certificates has introduced serious security concerns. Digital documents can be easily edited, duplicated, or forged using readily available tools, making it difficult to distinguish genuine certificates from fraudulent ones. This has led to a rise in cases of fake credentials, which not only undermine trust but also create challenges for institutions and employers attempting to verify authenticity.

Existing verification methods are largely based on manual validation or centralized database systems. Manual processes are time-consuming and require significant human effort, especially when dealing with large volumes of documents. On the other hand, centralized systems, although faster, suffer from limitations such as single points of failure, vulnerability to cyberattacks, and the risk of unauthorized data modification. These challenges

Doi:10.48047/ijiee.2026.16.1.10

highlight the need for a more secure, transparent, and efficient verification mechanism.

Blockchain technology has emerged as a promising solution to address these issues. It is a distributed ledger system that operates without a central authority and ensures that all recorded data is permanent and tamper-resistant. Each transaction in a blockchain is cryptographically linked to the previous one, forming a secure chain of records. This structure makes it extremely difficult to alter stored information without detection, thereby providing a high level of data integrity and trust.

In addition to blockchain, cryptographic hashing techniques play a vital role in ensuring document security. Hash functions generate a fixed-length digital fingerprint for any input data, and even the slightest modification in the input produces a completely different hash value. This property makes hashing highly effective for detecting changes in digital documents.

In this context, this paper presents **B-LOCK**, a blockchain-based certificate validation system designed to enhance the reliability and efficiency of academic document verification. The system generates a unique SHA-256 hash for each uploaded certificate and securely stores it on the blockchain. During verification, the system recalculates the hash of the submitted document and compares it with the stored value to determine authenticity.

Furthermore, the proposed system incorporates mechanisms for duplicate detection and role-based access control, ensuring that only authorized users can perform validation actions. By integrating blockchain technology with cryptographic hashing, the system provides a robust framework for preventing forgery, detecting tampering, and improving overall trust in digital certificate verification.

The primary objective of this study is to develop a secure, scalable, and user-friendly system that minimizes reliance on manual verification processes while ensuring high levels of accuracy, transparency, and data integrity in academic credential validation.

2. LITERATURE SURVEY

Smith et al. (2022) [1] proposed a blockchain-based academic credential verification system where universities directly issue certificates as blockchain transactions. Their approach improved data integrity but required institutions to adopt blockchain infrastructure at the issuance stage, which limits immediate practical adoption.

Gupta and Sharma (2023) [2] developed a decentralized document verification model that used cryptographic signatures and distributed ledgers. Their work demonstrated that blockchain can effectively prevent document tampering. However, the system focused mainly on certificate issuance and did not include workflow-based validation processes.

Rahman et al. (2024) [3] presented a smart contract-based certificate verification system for educational institutions. Their model allowed organizations to verify credentials automatically using blockchain records. Although the system reduced verification time, it required complex blockchain integration and specialized infrastructure.

Lee et al. (2023) [4] used SHA-256 hashing to detect document duplication in secure file storage systems. Their work showed that cryptographic hashing is effective in identifying identical documents but did not integrate the method with blockchain-based immutability.

Baldi et al. (2019) [5] conducted a security-focused study on blockchain-based protocols for academic credential certification. Their work highlighted how blockchain can ensure data integrity and prevent unauthorized modifications through cryptographic mechanisms. However, the study primarily emphasized theoretical security analysis and did not provide a complete implementation framework for real-world verification systems.

Rahman et al. (2023) [6] introduced *Verifi-Chain*, a blockchain-enabled credential verification system integrated with IPFS for decentralized storage. Their approach improved document availability and security by distributing data across multiple nodes. Despite these advantages, the system involves complex integration of multiple technologies, which may increase implementation difficulty and limit ease of adoption.

Andrade et al. (2026) [7] proposed a decentralized certificate issuance system based on smart contracts deployed on the TRON blockchain network. The model enables automated certificate generation and verification without intermediaries, enhancing transparency and efficiency. However, it requires institutions to adopt blockchain-based issuance processes, which may not be feasible for all organizations.

Gangwar et al. (2024) [8] developed a blockchain-based authentication system that incorporates QR codes for certificate verification. In this approach, each certificate is linked to a unique QR code that can be scanned to retrieve verification details from the blockchain. While the method simplifies the verification process, it mainly focuses on access

Doi:10.48047/ijiee.2026.16.1.10

convenience and may not fully address advanced security concerns such as duplication detection and workflow-based validation.

3.PROPOSED METHODOLOGY

The B-LOCK system is designed as a web-based platform that ensures secure and efficient certificate verification using blockchain technology. Users can upload certificates through a simple interface, and the system generates a unique hash value for each document. This hash functions as a digital fingerprint, meaning that even the smallest change in the file results in a completely different hash.

The generated hash is stored in a blockchain, where each block is securely linked to the previous one.

This structure guarantees that once data is recorded, it cannot be altered without detection.

During the verification process, authorized users upload a certificate, and the system recalculates its hash. This newly generated hash is compared with the value stored in the blockchain. A match confirms that the certificate is authentic, while a mismatch indicates possible tampering.

This method significantly reduces manual effort and improves the speed, reliability, and transparency of certificate validation.

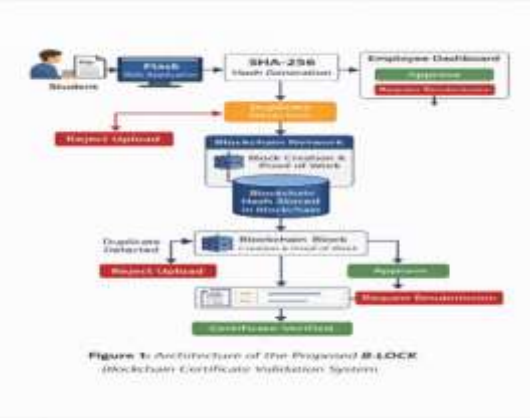

Figure 1: Architecture of the Proposed B-LOCK (Blockchain Certificate Validation System)

A .Certificate Upload and Hash Generation

When a user uploads a certificate, the system processes the file and generates a SHA-256 hash value. This hash acts as a unique identifier for the document. Even a minor change in the file produces a completely different hash.

The generated hash is stored along with relevant certificate details such as student name, certificate type, and timestamp.

B. Blockchain Storage

The generated hash is stored in a blockchain structure where each block contains:

- Block index
- Timestamp
- Previous block hash
- Certificate hash
- Nonce (for Proof-of-Work)

This structure ensures that once data is recorded, it cannot be modified without detection.

C. Duplicate Detection

To prevent redundancy, the system checks whether the generated hash already exists in the database. If a match is found, the upload is rejected, ensuring that duplicate certificates are not stored.

D. Certificate Verification and Approval

Authorized personnel can access uploaded certificates through a dashboard. They can review the document and decide whether to approve or request resubmission.

During verification, the system recalculates the hash of the uploaded certificate and compares it with the stored blockchain value:

- If both hashes match → certificate is valid
- If hashes differ → certificate is flagged as tampered

This process ensures accurate and reliable validation.

4.PERFORMANCE ANALYSIS AND RESULTS

The proposed B-LOCK blockchain certificate validation system was implemented using a Flask web application with blockchain-based storage for certificate hashes. The system was tested with multiple certificate uploads to evaluate its functionality, security, and verification performance. The following figures illustrate the system interface, blockchain storage process, and verification performance.

A. Student Certificate Details Upload Interface

Doi:10.48047/ijiee.2026.16.1.10

Figure 2: Student Certificate details Upload Interface

Figure 2 illustrates the interface designed for students to upload their certificates. In this module, users are required to provide details such as name, roll number, degree, and certificate type before submitting the document.

Once the certificate is uploaded, the system generates a SHA-256 hash value, which acts as a unique digital identifier. This hash is then securely stored within the blockchain, ensuring that the document remains tamper-proof.

B. Employee Verification Dashboard

The employee dashboard used for reviewing submitted certificates.

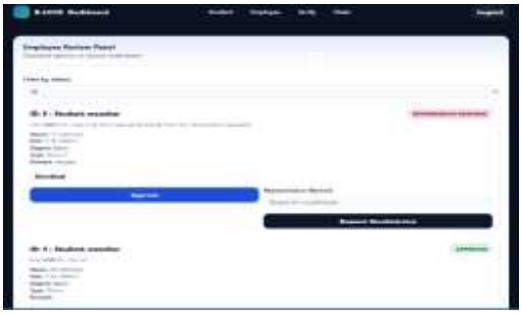

Figure 3: The employee dashboard used for reviewing submitted certificates

Figure 3 represents the dashboard provided to authorized personnel for reviewing submitted certificates. Through this interface, employees can access uploaded documents, examine their details, and verify their authenticity.

Based on the verification results, employees can either approve the certificate or request resubmission if discrepancies are found. This adds an additional layer of validation to the system.

C. Blockchain Storage

The blockchain ledger that stores certificate hash values.

Figure 4 illustrates the blockchain ledger utilized for storing certificate hash values in the proposed B-LOCK system. In this architecture, each certificate uploaded to the system is processed to generate a unique SHA-256 hash, which is then recorded as a transaction within a blockchain block.

Each block in the blockchain contains several critical components, including the block index, timestamp, certificate hash, previous block hash, and a nonce value used in the Proof-of-Work consensus mechanism. The inclusion of the previous block hash ensures that all blocks are cryptographically linked, forming a continuous and secure chain of records.

This interconnected structure provides immutability, which is a key feature of blockchain technology. Any attempt to modify the data within a block would result in a change in its hash value, thereby breaking the link with subsequent blocks. Such inconsistencies are immediately detectable, making unauthorized modifications practically infeasible.

Furthermore, the decentralized nature of blockchain storage enhances system reliability by eliminating dependence on a single centralized authority. Even if one node is compromised, the integrity of the overall system remains unaffected due to distributed validation.

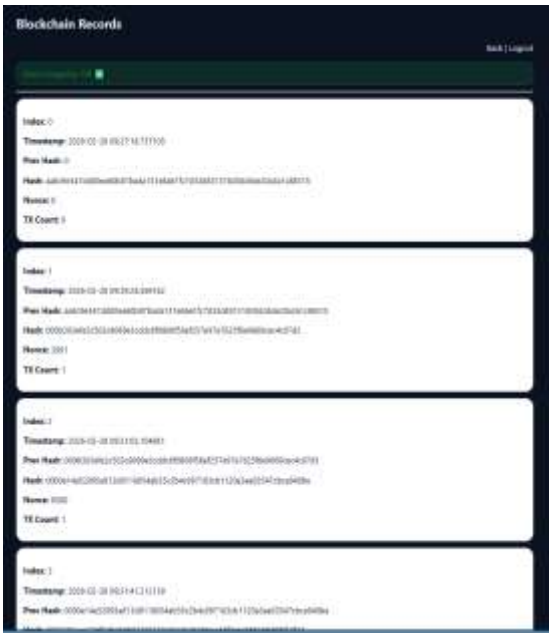

Figure 4: Blockchain Ledger Showing Stored Certificate Hashes

D. Certificate Verification Using the Verify Button

The certificate verification process using the Verify button in the system.

Doi:10.48047/ijiee.2026.16.1.10

Figure 5: Certificate Verification Process Using the Verify Button in the B-LOCK System.

Figure 5 demonstrates the certificate verification functionality within the system. During verification, a user uploads a certificate, and the system generates a new SHA-256 hash for the document.

This newly generated hash is compared with the hash stored in the blockchain:

- If both values match, the certificate is confirmed as authentic
- If there is a mismatch, the document is flagged as altered or invalid

This process ensures accurate and reliable validation of certificates.

E. System Performance Analysis

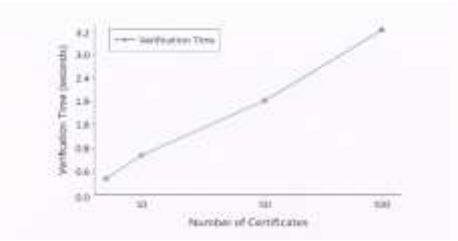

Figure 6: Verification Time for Different Numbers of Certificates

Figure 6 illustrates the performance analysis of the proposed B-LOCK system by depicting the relationship between the number of certificates processed and the corresponding verification time. This evaluation was conducted to measure the efficiency, scalability, and responsiveness of the system under varying workloads.

During testing, multiple certificates were uploaded and verified in sequence to observe how the system performs as the data volume increases. The verification process includes generating the SHA-256 hash of the uploaded certificate, retrieving the stored hash from the blockchain, and performing a comparison to validate authenticity.

The results show that the system maintains stable and consistent performance even as the number of certificates increases. Although a gradual increase in verification time is observed with higher input sizes, the growth rate remains minimal and within acceptable limits. This indicates that the system is capable of handling larger datasets without significant performance degradation.

.

5.CONCLUSION AND FUTURE WORK

A. Conclusion

This paper presented B-LOCK, a blockchain-based certificate validation system designed to improve the security and reliability of academic document verification. The proposed approach integrates SHA-256 hashing with blockchain storage and role-based access control to ensure that uploaded certificates remain secure and tamper-resistant.

The system generates a unique hash for each certificate and stores it within a blockchain structure, making any unauthorized modification easily detectable. Experimental evaluation shows that the system can successfully identify duplicate submissions as well as detect alterations in previously stored documents. Additionally, the inclusion of an employee verification interface provides an extra layer of validation, enhancing the overall trustworthiness of the system.

Overall, the results demonstrate that the combination of blockchain technology and cryptographic hashing offers a robust, transparent, and efficient solution for preventing certificate forgery and improving digital credential verification.

B. Future Work

Although the proposed B-LOCK system provides a secure framework for certificate validation, several enhancements can be implemented to further improve its functionality and scalability:

1. Institutional Digital Signatures
   Future versions of the system can incorporate digital signatures issued by universities or educational institutions. This would enable dual

   verification, combining blockchain-based validation with institutional authentication for higher reliability.

2. Advanced Forgery Detection Using Machine Learning
   Machine learning techniques can be integrated to detect visual tampering in certificates, such as altered text, modified

Doi:10.48047/ijiee.2026.16.1.10

marks, or inconsistent formatting in images and PDF documents.

3. Mobile-Based Verification Application
A dedicated mobile application can be developed to allow employers and institutions to verify certificates quickly using smartphones, improving accessibility and ease of use.

4. Multi-Institution Blockchain Network
The system can be expanded into a shared blockchain network that supports multiple institutions. This would enable cross-institution certificate verification and enhance scalability for large-scale adoption.

REFERENCES

[1] M. Baldi, F. Chiaraluce, M. Kodra and L. Spalazzi, "Security analysis of a blockchain-based protocol for the certification of academic credentials," *IEEE Access*, 2019. [Online]. Available: https://arxiv.org/abs/1910.04622

[2] T. Rahman, S. I. Mouno, A. M. Raatul, A. K. Al Azad and N. Mansoor, "Verifi-Chain: A credentials verifier using blockchain and IPFS," *arXiv Preprint*, 2023. [Online]. Available: https://arxiv.org/abs/2307.05797

[3] A. J. E. Andrade and F. C. Amate, "A decentralized academic certificate issuance system using smart contracts on the TRON network," *arXiv Preprint*, 2026. [Online]. Available: https://arxiv.org/abs/2601.08513

[4] S. Gangwar and A. Chaurasia, "Blockchain-based authentication and verification system for academic certificates using QR codes," *International Journal of Computer Applications*, 2024. [Online]. Available: https://www.researchgate.net/publication/382085901_Blockchain-based_Authentication_and_Verification_System_for_Academic_Certificate_using_QR_Code_and_Decentralized_Applications

[5] H. Liu, J. Han and Y. Wang, "Blockchain-based certificate verification system for academic credentials," *IEEE Access*, vol. 8, pp. 215741-215750, 2020.

[6] R. Arenas and P. Fernandez, "CredenceLedger: A permissioned blockchain for verifiable academic credentials," *2018 IEEE International Conference on Engineering, Technology and Innovation*, pp. 1-6, 2018.

[7] J. Gresch, B. Rodrigues, E. Scheid, S. Kanhere and B. Stiller, "The proposal of a blockchain-based architecture for transparent certificate handling," *Lecture Notes in Business Information Processing*, Springer, 2019.

[8] A. Tariq, H. B. Haq and S. T. Ali, "Cerberus: A blockchain-based accreditation degree verification system," *IEEE Transactions on Computational Social Systems*, 2023.

[9] O. Saleh, O. Ghazali and M. E. Rana, "Blockchain-based framework for educational certificate verification," *Journal of Critical Reviews*, vol. 7, pp. 79-84, 2020.

[10] N. Nguyen, T. Dao and B. Do, "Towards a blockchain-based certificate authentication system," *PeerJ Computer Science*, 2020.

[11] A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "A systematic literature review on blockchain-based systems for academic certificate verification," *IEEE Access*, 2023.

[12] P. Gundgurti, "Smart and secure certificate validation system through blockchain," *International Journal of Computer Science and Network Security*, 2020.

[13] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[14] Flask Development Team, "Flask Web Framework Documentation," [Online]. Available: https://flask.palletsprojects.com

Doi:10.48047/ijiee.2026.16.1.10