IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.141274

Blockchain Based Identity Verification System

Ms. Kavitha K S[1], K Pramod Kumar[2], Hemanth R[3], Harish R A[4], G Sharath Raj[5]

Department of Computer Science and Engineering, K S School of Engineering and Management, Bengaluru, Karnataka, India[1-5]

Abstract: In today's digital environment, ensuring that academic and professional documents are genuine has become increasingly difficult, especially with the growing incidents of tampering and forgery. The proposed Blockchain-Based Identity Verification System offers a secure and transparent method for issuing and validating digital certificates. By storing certificate information on the blockchain, the system guarantees immutability—once a certificate is recorded with its unique ID, it cannot be altered or replicated [1].

IPFS further enhances the system by providing decentralized and reliable file storage [2]. Authorized institutions can issue certificates digitally, and verifiers such as recruiters or background-check teams can confirm their authenticity through a simple online verification portal, without depending on any intermediaries. This not only strengthens security and trust but also supports a shift toward paperless verification, reducing manual workload and environmental impact. Overall, the system aims to build a dependable digital credential ecosystem that benefits both educational institutions and employers.

Keywords: Blockchain, IPFS (Inter Planetary File System), decentralized storage, Identity verification

I. INTRODUCTION

Increased demands for secure and efficient certificate verification have emerged with the increased usage of digital credentials. Traditional solutions mostly depend on physical documents or centralized databases, paving the way for document forgery, unauthorized changes, and administrative delays [3]. As an organization expands its digital infrastructure, there arises a pressing need for a transparent, trustable, and automated verification mechanism [4].
Blockchain is highly suitable for applications where permanent and tamper-proof data storage is required because of its decentralized and immutable ledger structure. Along with the use of decentralized storage technologies like IPFS, institutions can then issue certificates that can be verified through cryptographic proofs instead of having to manually check their veracity. This, therefore, eliminates the problem of fraudulent certificates and reduces dependence on intermediaries.
This research proposes a system that will securely store the metadata of the certificates on a blockchain network, whereas the actual certificate files will be distributed via IPFS. Each certificate has a unique hash associated with it for proving authenticity. A verifier can instantly check the validity of any certificate with ease via a simple verification interface. With the introduction of automation, transparency, and decentralization, the solution aims at building a robust digital credential ecosystem in the academic and professional landscape.

II. RELATED WORK

There are numerous digital credentialing systems, but the vast majority rely on centralized databases that are at the mercy of corruption and single-point failures. Other institutions have utilized QR-based verification, which allows for convenience of access, but is ultimately dependent on central authority verification. Academic credential blockchain systems, such as Blockcerts, have shown the capabilities of decentralized verification, but due to complexity and previous blockchain storage limitations, adoption has been limited [5].
This study aims to bridge the gap by combining blockchain with IPFS and thus overcome storage limitations to provide scalability, cost efficiency, and greater security than previous approaches.

III. PROBLEM STATEMENT

The verification of certificates is a problem most educational and professional institutions face.
The major challenges are:

- High risk of certificate forgery and document manipulation [3].
- Delayed verification due to manual processing.
- Lack of transparency in verification workflows.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025
DOI: 10.17148/IJARCCE.2025.141274

- ❖ Dependence on centralized systems prone to data breaches or system failures [4].
- ❖ High administrative workload and paper-based documentation problems.

A decentralized, tamper-proof, and automated verification system is required to overcome these limitations.

IV. OBJECTIVES

The main objectives of this research are:

1. **Ensure Tamper-Proof Storage of Certificates:** Blockchain ensures that once certificates are recorded, they cannot be modified or deleted, maintaining authenticity and preventing forgery [1].
2. **Provide Decentralized File Storage:** Using IPFS for decentralized storage eliminates single points of failure, ensuring data integrity, availability, and security [2].
3. **Enable Secure Verification:** Certificates can be verified through their unique blockchain hash, allowing instant and trustworthy validation without intermediaries.
4. **Empower Users with Credential Ownership:** Users gain complete control over their digital certificates, enabling them to store, share, and manage credentials securely.
5. **Reduce Dependency on Centralized Authorities:** The system operates without relying on a central authority, enhancing transparency, trust, and reliability in the verification process.

V. SYSTEM ARCHITECTURE

A. System Components

The proposed system consists of the following components:

1. **Issuer(College/Organization):** Issues certificates, uploads them to IPFS, and stores the certificate hash on blockchain.
2. **Blockchain Network:** Stores immutable certificate metadata such as certificate ID, issuer ID, timestamp, and IPFS hash [1].
3. **IPFS Storage:** Provides decentralized storage for certificate files [2].
4. **Verifier (Company/Organization):** Uses the verification portal to validate certificates by matching hash values.
5. **User/Certificate Holder:** Receives a unique certificate ID, Encryption Key and shares it with verifiers.

B. Workflow

- ❖ Institution uploads certificate → IPFS generates a unique file hash.
- ❖ Smart contract records metadata and file hash on blockchain.
- ❖ Certificate holder receives certificate ID and verification link.
- ❖ Verifier enters the certificate ID on the portal.
- ❖ System retrieves blockchain record → compares stored hash with IPFS file hash.
- ❖ If hash matches → certificate is verified as authentic.

VI. METHODOLOGY

A. Blockchain Layer

- Implemented on Ethereum or a private blockchain such as Ganache.
- Smart contracts written in Solidity.
- Stores certificate metadata and IPFS hash [1].

B. IPFS Storage

- Used to store certificate PDFs securely.
- Returns a unique content identifier (CID).
- Ensures file integrity and decentralized availability[2].

C. User Interface

- Web application built using HTML, CSS, JavaScript
- Issuer portal for certificate issuance.
- verification page for verifiers.

D. Security Considerations

- Hashing using SHA-256 for integrity checks [3].

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.141274

- No direct file stored on blockchain to minimize cost.
- Smart contract access restricted to authorized issuers.

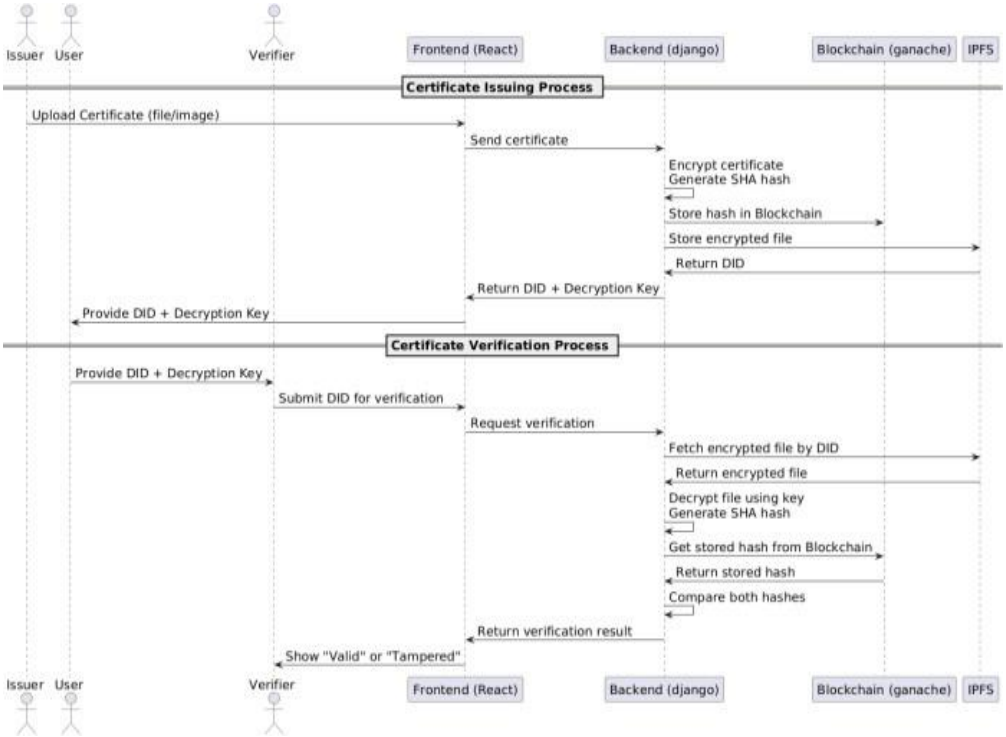

Fig. 1. Sequence diagram.

1. Encrypt certificates, generate hash, and store hash on Blockchain.
2. Store encrypted certificates on IPFS and generate DID.
3. Fetch file via DID, decrypt with key, and match hash with Blockchain.
4. Give users DID and key so they control sharing of certificates.
5. Use Blockchain smart contracts and IPFS to allow independent verification.

VII. RESULTS AND DISCUSSION

The system was tested with sample academic certificates and successfully demonstrated:
Testing with sample academic certificates showed:

- Verification time < 5 seconds.
- Tampering instantly detectable via hash mismatch [4].
- Reduced administrative workload.
- Lower storage cost due to hash-only blockchain storage [5].

1. **Instant Verification:** Verifiers were able to check authenticity in less than 5 seconds.
2. **Tamper-Proof Storage:** Any modification to certificates changed the IPFS hash, making tampering detectable.
3. **Reduced Administrative Effort:** Institutions reported reduced manual verification workload.
4. **Scalability:** Storing hashes on blockchain instead of files significantly lowered storage costs.

VIII. CONCLUSION

This paper presents a robust and scalable Blockchain-Based Identity Verification System that addresses the limitations of traditional certificate validation. By integrating blockchain and IPFS, the system ensures secure issuance, decentralized storage, and instant verification of academic and professional documents. The solution enhances trust, reduces administrative complexity, prevents forgery, and supports environmentally responsible, paperless operations. Future enhancements may revocation and update feature, include multi-institution interoperability, biometric-based identity binding, and mobile-based verification

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.141274

ACKNOWLEDGMENT

The authors acknowledge the support of faculty mentors, technical advisors, and all contributors involved in the development and testing of the proposed system.

REFERENCES

[1]. V. Nehra, A. M. J., H. Khanna and N. Jindal, "Decentralized Digital Identity Verification System Using Blockchain Technology," *2024 4th International Conference on Innovation Practices in Technology and Management (ICIPTM)*, Noida, India, 2024, pp. 1-6.

[2]. Jamal, A. S. N. Syahirah, R. A. A. Helmi, and M.-A. Fatima "Blockchain-Based Identity Verification System," *Faculty of Information Sciences and Engineering, Management & Science University*, Shah Alam, Malaysia.

[3]. G. Malik, K. Parasrampuria, S. P. Reddy, and S. Shah, "Blockchain Based Identity Verification Model," *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, 2019, pp. 1–6.

[4]. S. Srivastava, D. Agarwal and B. Chaurasia, "Secure Decentralized Identity Management using Blockchain," *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Exeter, UK, 2023, pp. 1355–1360.

[5]. R. S. Barpanda, R. N. Mohapatra, and S. Kumar, "Digital Identity System Using Blockchain-based Self-Sovereign Identity and Zero Knowledge Proof," *2023 21st OITS International Conference on Information Technology (OCIT)*, Bhubaneswar, India, 2023, pp. 611– 616.

