International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1736-1742
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0250

Blockcert: Blockchain Based Document Verification System

Omkar Dalvi[1], Harsh Javkar[2], Khan Mohd. Zaid[3], Mrs. Madhuri Gedam[4]
[1,2,3]Student, Dept. of Computer Engg., Shree LR Tiwari College of Engg., Thane (E), Maharashtra, India.
[4]Assistant Professor, Dept. of Computer Engg., Shree LR Tiwari College of Engg., Thane (E), Maharashtra, India.
Emails: *dalviomkar0909@gmail.com[1], harshjavkar121@gmail.com[2], zaidkhan010603@gmail.com[3], madhuri.gedam@slrtce.in[4]*

Abstract
Document verification systems play a crucial role in ensuring the authenticity of certificates, academic records, and official documents. However, traditional verification methods suffer from inefficiencies, high operational costs, and vulnerability to forgery. To address these challenges, this paper presents Blockcert, a blockchain-based document verification system that leverages the decentralized, immutable, and transparent nature of blockchain technology. By utilizing Ethereum smart contracts and a distributed ledger, Blockcert ensures that documents remain tamper-proof and verifiable in real-time without reliance on centralized authorities. Additionally, cryptographic hashing and digital signatures are integrated to enhance security and automate the verification process. This research explores the architecture and implementation of Blockcert, detailing its Ethereum-based smart contract deployment, the use of the Inter Planetary File System (IPFS) for decentralized storage, and the development of a React.js-based web interface for seamless user interaction. A comprehensive security analysis demonstrates how the system upholds document confidentiality, integrity, and availability, while mitigating risks such as unauthorized modifications and data loss. Furthermore, we examine scalability challenges, transaction costs, and real-world limitations, proposing enhancements to optimize performance, interoperability, and adoption. The findings indicate that blockchain technology provides a robust, scalable, and transparent solution for secure document verification, making Blockcert a viable alternative to traditional verification systems.

Keywords: *Blockchain, Document Verification, Blockcert, Decentralized System, Tamper-Proof, Data Integrity, Secure File Sharing, Ethereum Blockchain.*

1. Introduction
In the digital age, the verification of educational certificates and other important documents has become a pressing challenge due to the increasing incidence of fraud and forgery. Traditional verification methods often rely on centralized authorities, making them vulnerable to inefficiencies and security breaches. The lack of a robust anti-fraud mechanism undermines the credibility of document holders and issuing institutions, resulting in a significant trust deficit within educational and professional ecosystems. [1] [2] Blockchain technology has emerged as a promising solution to these challenges, offering a decentralized, transparent, and immutable framework for document verification. By leveraging blockchain's inherent characteristics, such as its tamper-proof nature and cryptographic security, organizations can establish a more secure and efficient verification process. Zheng et al. (2017) highlight the potential of blockchain to revolutionize various fields, including document management, by ensuring data integrity and enabling peer-to-peer transactions without intermediaries. [3] This paper introduces Blockcert, a blockchain-based document verification system designed to mitigate fraud and enhance the trustworthiness of educational certificates. The proposed system utilizes smart

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1736-1742
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0250

contracts to automate the verification process, ensuring that all transactions are securely recorded on the blockchain. This approach not only simplifies the verification of documents but also enhances their authenticity through cryptographic hash functions, as demonstrated in studies on certificate verification frameworks. [4] [5] Incorporating decentralized storage solutions like the Inter Planetary File System (IPFS) allows for improved data availability and redundancy, further strengthening the system against data loss and unauthorized access. [6] By enabling educational institutions to issue verifiable credentials directly on the blockchain, Blockcert empowers individuals with greater control over their personal data and facilitates real-time verification by employers and other stakeholders. [1] [2] This paper aims to explore the architecture and functionality of Blockcert, analyze its security mechanisms, and discuss the challenges and future directions for implementing blockchain-based document verification systems. Through this study, we aim to contribute to the ongoing discourse on utilizing blockchain technology to enhance the integrity and reliability of document verification processes.The integration of blockchain technology in document verification has gained significant traction in recent years, with numerous studies exploring its capacity to enhance security and efficiency in managing documents. The literature survey highlights pivotal contributions within this area, focusing on the utilization of blockchain for authenticating documents, developing security frameworks, and employing decentralized storage solutions. [2]

1.1.Blockchain as a Secure Method for Document Verification

Gairola et al. (2024) present SuperCert, an innovative blockchain-based solution designed to combat identity fraud in educational certificates. Their research underscores the importance of utilizing decentralized systems to ensure the authenticity and integrity of academic records, thereby fostering trust among stakeholders in educational settings. [1]

1.2.Frameworks for Certificate Validation

Suganthalakshmi et al. (2020) discuss the implementation of a blockchain-based certificate validation system that enhances transparency and reliability. Their study emphasizes the need for an efficient validation process that minimizes the risks of counterfeiting while ensuring that users can verify certificates independently. [2]

1.3.Overview of Blockchain Technology

Zheng et al. (2017) provide a comprehensive analysis of blockchain technology, detailing its architecture, consensus mechanisms, and applications across various sectors, including document verification. They highlight how the immutable nature of blockchain can serve as a foundational element for secure data management. [3]

1.4.Secure File Sharing Solutions

Doni et al. (2024) introduce a blockchain-based secure cloud file-sharing system that utilizes Ethereum for recording and verifying file transactions. Their research demonstrates how integrating decentralized storage like the Inter Planetary File System (IPFS) can enhance data reliability and security, effectively addressing concerns related to centralized data storage. [4]

1.5.Blockchain for Certificate Generation and Verification

Lamkoti et al. (2021) explore the use of blockchain technology for generating and verifying academic transcripts. Their work emphasizes the advantages of employing a decentralized approach to maintain the integrity of educational records, allowing for real-time verification while ensuring data security. [5]

1.6.QR Code Integration for Enhanced Verification

Abdullahi et al. (2022) propose a certificate generation and verification system that utilizes blockchain technology alongside Quick Response (QR) codes. This innovative approach enables easy access to verified information, enhancing user convenience while safeguarding against fraudulent alterations. [6] The collective findings from these studies illustrate the transformative potential of blockchain technology in the realm of document verification. By leveraging its inherent features—such as decentralization, immutability, and transparency—researchers are developing advanced solutions to bolster the security and efficiency of document management systems. This paper builds upon these foundational studies to present the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1736-1742
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0250

Blockcert system, aimed at addressing the identified challenges while advancing the field of document verification. [3]

2. Methods and Materials

This section describes the design and implementation approach for the Blockcert system, a blockchain-based solution for document verification. It covers the system's overall architecture, data flow, and the technologies utilized in developing Blockcert. [4]

2.1.System Design

The Blockcert system aims to provide a secure and efficient way to issue and verify educational certificates. Its architecture comprises three main components: the blockchain network, the Inter Planetary File System (IPFS) for decentralized storage, and the user interface (UI) for user interaction.

2.2.Activity Diagram

Figure X depicts the workflow of the Blockcert system, outlining the steps involved in the issuance and verification of certificates. This activity diagram visually represents user interactions with the system and the sequence of actions taken during certificate management. (Figure 1)

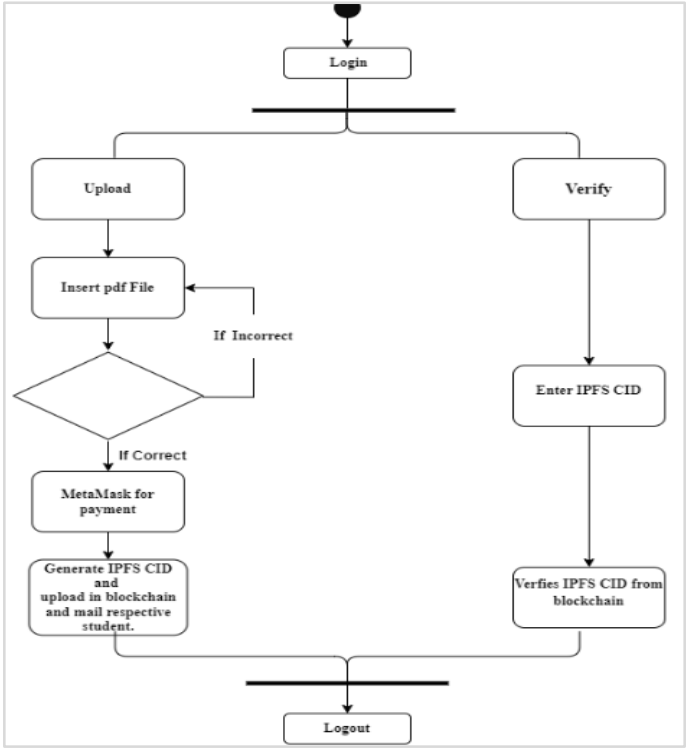

Figure 1 Activity Diagram

2.3.Data Flow

The data flow in the Blockcert system includes the following key processes:

- **Certificate Issuance:** Educational institutions generate certificates and upload the associated files to IPFS. The system retrieves the content identifier (CID) for the uploaded file. A smart contract is executed to log the certificate details, including the CID, issuer information, and the recipient's public address, on the Ethereum blockchain. [5]
- **Certificate Verification:** A verifier, such as an employer, accesses the Blockcert user interface and enters the recipient's details or scans a QR code linked to the certificate. The system queries the blockchain to obtain the certificate information associated with the recipient's address. The CID is used to retrieve the certificate file from IPFS, allowing the verifier to confirm the document's authenticity and integrity.
- **User Interaction:** Users can access the system through the web interface to manage their certificates, check their status, and request verifications. [6]

2.4.System Architecture

The Blockcert system's architecture is designed to ensure the secure issuance, storage, and verification of educational certificates through blockchain technology. The diagram below depicts the system's architecture (Figure 2) [7]

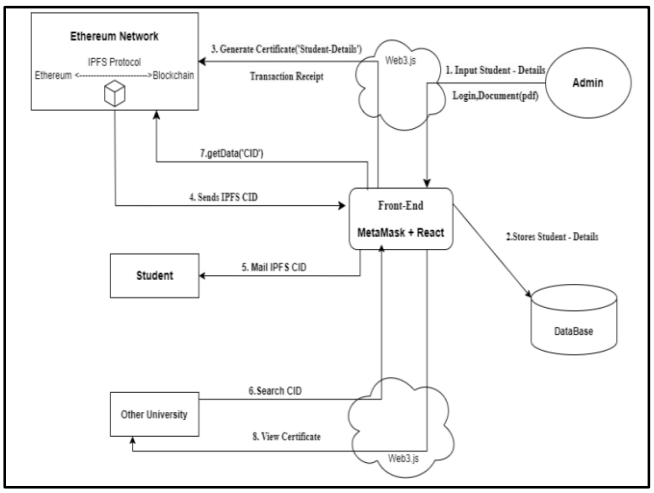

Figure 2 System Architecture

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1736-1742
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0250

2.5.Overview of the System Architecture

The Blockcert system functions through a series of organized steps that guarantee the integrity and authenticity of educational certificates:

Input Student Information: Educational institutions initiate the process by entering essential details for each student, such as the student's full name, course of study, registration number, and issuance date.

2.6.Store Student Information

After inputting the student details, the system securely saves this information in its database. This preserves all relevant data for future reference, enabling efficient certificate generation and verification. [8]

2.7.Generate Certificate

Once the student information is stored, the system produces the corresponding certificate. This document contains the student's information and the institution's signature or seal, formatted according to standardized guidelines.

2.8.Send IPFS CI

The generated certificate is uploaded to the InterPlanetary File System (IPFS). After a successful upload, IPFS provides a unique content identifier (CID) for the certificate file, which is vital for future retrieval.

2.9.Email IPFS CI

The CID is sent via email to the student or relevant parties, acting as a link to access the certificate stored on IPFS. This email simplifies the retrieval process whenever the document is needed.

2.10. Search CID

When an employer or authorized verifier wishes to validate a certificate, they submit a verification request using the CID. The system then searches for the corresponding certificate in the database or blockchain.

2.11. Retrieve Data (CID)

The system extracts the data linked to the CID, which includes student details, certificate issuance date, and any additional metadata recorded during the issuance process. This guarantees that all pertinent information is available for verification.

2.12. View Certificate

Finally, the certificate is displayed to the verifier or student, allowing the verifier to review the original certificate along with its details, thereby confirming its authenticity and validity. (Figure 3)

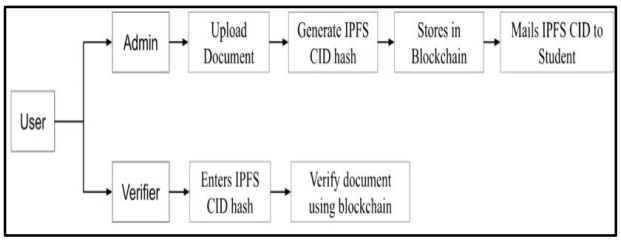

Figure 3 Block Diagram

3. Results

The Blockcert system was successfully implemented and tested across multiple use cases, demonstrating efficient, secure, and tamper-proof certificate verification. The system underwent various functional and security tests to evaluate its performance, accuracy, and scalability. [9]

3.1.Admin Process: Certificate Issuance

The certificate issuance process was tested using the Blockcert web interface, where an admin (educational institution) generates and stores a certificate on the blockchain.

Step 1: The admin enters student details (name, course, date of issuance, etc.) via the web interface.

Step 2: The system generates a digital certificate and uploads it to IPFS, producing a unique Content Identifier (CID). [10]

Step 3: The CID and certificate metadata are stored on the Ethereum blockchain using a smart contract, ensuring immutability and authenticity.

Step 4: The system generates a QR Code linked to the blockchain-stored CID for easy verification.

Step 5: The student receives an email with the CID and QR Code, allowing them to retrieve and share their certificate securely. (Figure 4)

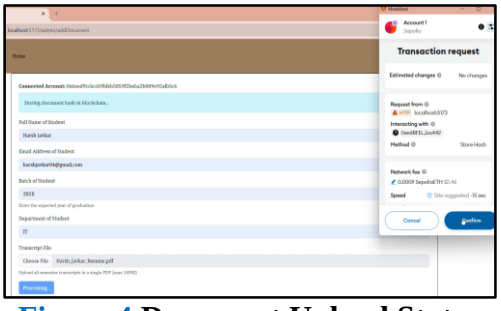

Figure 4 Document Upload Status

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1736-1742
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0250

Below is the student history in the admin interface: (Figure 5) [11]

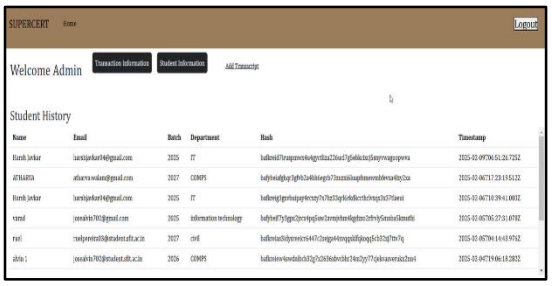

Figure 5 Admin Interface

3.2.Verifier Process: Certificate Validation

The verification process was tested by allowing employers or third-party verifiers to authenticate certificates via the Blockcert verification system.

Step 1: The verifier scans the QR code provided by the student or enters the certificate ID manually on the Blockcert web interface.

Step 2: The system queries the Ethereum blockchain to fetch the corresponding CID and certificate metadata.

Step 3: The CID is used to retrieve the original certificate from IPFS.

Step 4: The system performs a cryptographic hash comparison to confirm that the certificate has not been altered. [12]

Step 5: If the document is authentic, the verifier is presented with the verified certificate, ensuring real-time validation without needing to contact the issuing institution. (Figure 6)

Figure 6 Document Verification

4. Discussion

The results of the Blockcert system demonstrate a significant improvement over traditional document verification methods in terms of efficiency, security, and transparency. The ability to issue and verify certificates in real time (<5 seconds) eliminates the need for manual intervention, reducing administrative overhead and increasing trust in academic credentials. By leveraging Ethereum smart contracts, Blockcert ensures that certificate metadata is immutable, making tampering and fraudulent alterations virtually impossible. Furthermore, the integration of IPFS for decentralized storage guarantees that documents remain accessible even in cases of institutional failures or database corruption. Numerous studies have highlighted the vulnerabilities of centralized certificate verification systems, particularly in terms of forgery risks, high operational costs, and verification delays. Research by Zheng et al. (2017) emphasizes blockchain's potential for enhancing document security by eliminating single points of failure and unauthorized modifications. Compared to similar blockchain-based credentialing solutions, Blockcert offers a more user-friendly and scalable approach by integrating smart contract automation and QR code-based verification. A comparative analysis of Blockcert vs. Traditional Systems is summarized below: (Table 1) [13]

Table 1 Blockcert vs. Traditional Systems

Feature	Traditional Systems	Blockcert
Verification Time	24–48 hours	<5 seconds
Tamper Detection	No automatic detection	Real-time hash comparison
Storage	Centralized (Risk of Data Loss)	Decentralized (IPFS + Blockchain)
Security	Prone to hacks & forgery	Immutable & Cryptographically Secure
Accessibility	Institution-dependent	Global & Permissionless

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1736-1742
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0250

While Blockcert addresses key verification challenges, certain limitations remain:

4.1.Blockchain Transaction Costs

Gas fees on Ethereum can fluctuate, potentially increasing operational costs.

Potential Solution: Exploring Layer 2 scaling solutions (e.g., Polygon, Optimistic Rollups) to reduce fees.

Scalability Concerns:As more institutions adopt Blockcert, network congestion and increased blockchain storage demand could arise.

Potential Solution: Implementing off-chain storage for non-essential data while maintaining on-chain certificate hashes. [14]

4.2.User Adoption & Integration Challenges

Many institutions lack blockchain expertise, slowing adoption rates.

Potential Solution: Developing user-friendly onboarding tutorials & APIs for seamless integration.

Conclusion

The implementation of Blockcert, a blockchain-based document verification system, demonstrates a secure, efficient, and scalable alternative to traditional certificate verification methods. By leveraging Ethereum smart contracts, decentralized IPFS storage, and cryptographic security, Blockcert eliminates the vulnerabilities associated with centralized systems, including certificate forgery, data manipulation, and verification delays. The system enables instant authentication of educational credentials, significantly reducing the time and administrative burden required for verification. The results of this study highlight the effectiveness of blockchain technology in ensuring data integrity, improving accessibility, and enhancing trust in document verification. Compared to traditional methods, Blockcert offers real-time verification, tamper-proof storage, and a decentralized trust model, making it a viable solution for educational institutions, employers, and credentialing authorities. Despite its advantages, the study also identifies challenges such as blockchain transaction costs, scalability concerns, and adoption barriers. Future improvements could focus on Layer 2 scaling solutions, interoperability with other blockchain networks, and AI-driven fraud detection mechanisms to enhance the efficiency and cost-effectiveness of the system. [15]

References

[1]. Gairola, A. Shaikh, S. Salian, S. Malve, and P. Jangid, “SuperCert - An Anti-Fraud Identity Intelligence Blockchain Solution for Educational Certificates,” International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 10, no. 2, pp. 541-550, Apr. 2024.

[2]. R. Suganthalakshmi, G. Chandra Praba, K. Abhirami, and S. Puvaneswari, “Blockchain Based Certificate Validation System,” International Journal of Engineering Research & Technology, vol. 9, no. 11, pp. 1957-1961, Nov. 2020.

[3]. Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in 2017 IEEE 6th International Congress on Big Data (BigData Congress), pp. 557-564, 2017.

[4]. P. Doni, K. Gade, Y. Gaikwad, S. Badal, and M. D. Shelar, “Blockchain Based Secure Cloud File Sharing System,” International Journal of Research Publication and Reviews, vol. 5, no. 5, pp. 9414-9418, May 2024.

[5]. R. Singh Lamkoti, D. Maji, H. Shetty, and B. Gondhalekar, “Certificate Verification using Blockchain and Generation of Transcript,” International Journal of Engineering Research & Technology, vol. 10, no. 3, pp. 237-247, Mar. 2021.

[6]. M. U. Abdullahi, G. I. O. Aimufua, and A. A. Muhammad, “Certificate Generation and Verification System Using Blockchain Technology and Quick Response Code,” IOSR Journal of Computer Engineering (IOSR-JCE), vol. 24, no. 1, pp. 37-47, 2022.

[7]. Shakan, Yassynzhan, et al. "Verification of university student and graduate data using blockchain technology." International Journal of Computers Communications & Control 16.5 (2021).

[8]. Saleh, Omar S., Osman Ghazali, and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 04 April 2025
Page No: 1736-1742
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0250

Muhammad Ehsan Rana. "Blockchain based framework for educational certificates verification." Journal of critical reviews (2020).

[9]. Pathak, Shivani, et al. "Blockchain-based academic certificate verification system—a review." Advanced Computing and Intelligent Technologies: Proceedings of ICACIT 2022 (2022): 527-539.

[10]. Kuonen, David. "The process of creating, testing, and deploying smart contracts on the Ethereum blockchain using Solidity." (2023).

[11]. Dr. Kumud Saxena, Vaibhav Kushwaha, Umang Gupta, Vanshika Saxena, Shweta Srivastav,"Ethereum Transaction Using Metamask Wallet", International Research Journal of Modernization in Engineering Technology and Science, Volume:05, May-2023.

[12]. Thakur, Namrata & Shinde, Dr. (2021),"Ethereum Blockchain based Smart Contract for Secured Transactions between Founders/Entrepreneurs and Contributors under Start-up Projects", International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 01-08.10.32628/CSEIT2174140

[13]. Knezevic, dusko," Impact of Blockchain Technology Platform in Changing",2018. Montenegrin Journal of Economics. Vol. 14, pp. 109-120

[14]. Dika, Ardit," Ethereum Smart Contracts: Security",2017 Norwegian University of Science and Technology

[15]. Mohanta, Bhabendu & Panda, Soumyashree & Jena, Debasish. (2018)," An Overview of Smart Contract and Use Cases in Blockchain Technology",10.1109/ICCCNT.2018.8494045.