WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

BLOCKCHAIN BASED DIGITAL CERTIFICATE VERIFICATION SYSTEM

[1] Khushi Lalwani, [2]Chahal Dewangan, [3] Dr. Abha Choubey

[1 2] B.Tech students, Department of Computer Science Engineering Shri Shankaracharya Technical Campus, Bhilai Chhattisgarh
[3]Professor, Department of Computer Science Engineering Shri Shankaracharya Technical Campus, Bhilai Chhattisgarh

ABSTRACT :

In an era where credential forgery and document tampering are increasingly common, the need for a secure and verifiable system for issuing digital certificates is critical. This paper presents a decentralized application (DApp) that leverages blockchain technology to ensure the authenticity and integrity of digital certificates. Built using Ethereum smart contracts, IPFS for decentralized storage, and a React.js frontend, the system allows educational institutions to issue tamper-proof certificates and enables employers or third parties to instantly verify them without relying on a centralized authority. The certificate files are stored securely on IPFS, while their corresponding cryptographic hashes are recorded immutably on the blockchain. This dual-layer architecture ensures that any modification to the certificate can be easily detected. The system demonstrates significant improvements in transparency, efficiency, and trustworthiness over traditional verification methods, making it a viable solution for education, recruitment, and other sectors where credential verification is essential.

1. INTRODUCTION

In today's fast-paced digital era, the authenticity of credentials such as academic certificates, training records, and professional licenses plays a critical role in education, employment, and beyond. However, the traditional systems for issuing and verifying such documents are often centralized, inefficient, and vulnerable to forgery and tampering. Manual verification processes are time-consuming, require trust in intermediaries, and often suffer from a lack of transparency and standardization across institutions.

The growing instances of fake certificates and manipulated credentials pose a significant threat to institutional integrity and public trust. As educational institutions, companies, and governments move towards digital transformation, the need for a secure, tamper-proof, and decentralized solution for certificate management becomes more pressing.

Blockchain technology offers a promising solution to this problem. By utilizing the inherent properties of blockchain—immutability, decentralization, transparency, and security—it is possible to create a system where certificates can be issued, stored, and verified without the need for a central authority. Furthermore, integrating IPFS (InterPlanetary File System) for decentralized file storage allows large certificate files (e.g., PDFs) to be stored efficiently off-chain while still ensuring their authenticity via cryptographic hashing.

This paper introduces a Blockchain-Based Digital Certificate Verification System developed using Ethereum smart contracts, IPFS, and a modern web frontend. The proposed system allows institutions to issue certificates whose authenticity can be independently and instantly verified by any stakeholder, thereby minimizing fraud, reducing verification delays, and increasing public trust in digital credentials.

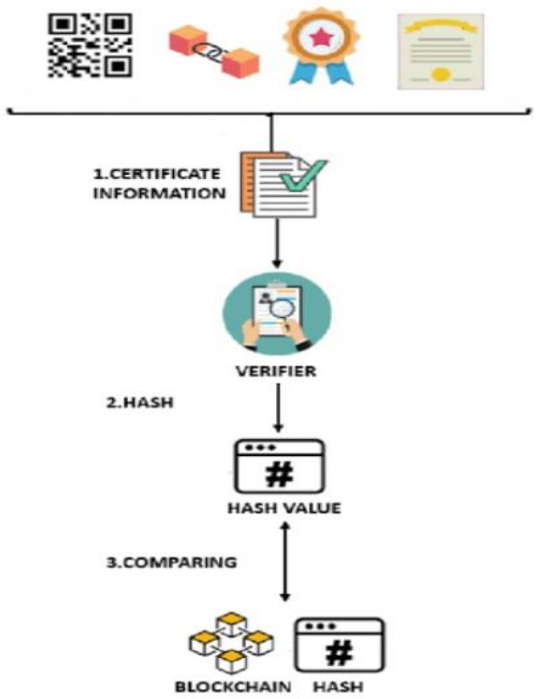
2. LITERATURE SURVEY

The verification of academic and professional certificates has traditionally relied on centralized authorities and manual processes, which are often inefficient, error-prone, and susceptible to forgery. In response to these challenges, blockchain technology has emerged as a promising solution for enhancing transparency, immutability, and decentralization in credential verification systems. Several studies have explored the use of blockchain for issuing, storing, and validating digital certificates. For instance, Grech and Camilleri (2017) discussed the application of blockchain in education, highlighting how platforms like Blockcerts enable institutions to issue tamper-proof academic credentials. Similarly, Turkanović et al. (2018) introduced EduCTX, a blockchain-based higher education credit platform, which demonstrated the feasibility of global academic credential standardization. These systems leverage the decentralized nature of blockchain to provide secure, verifiable records that can be accessed by third parties without relying on intermediaries.

Further literature supports the notion that blockchain can eliminate fraud in certificate issuance by ensuring each credential is cryptographically signed and publicly verifiable. IBM's research (2019) emphasized the role of smart contracts in automating certificate validation, reducing administrative overhead, and fostering trust among stakeholders. Moreover, blockchain-based verification aligns with the broader trends in digital identity management and self-sovereign identity, where users control and present their credentials without exposing unnecessary personal data. Despite these advantages, challenges remain in terms of scalability, user adoption, and integration with legacy systems. Studies by Zhao et al. (2020) and Nguyen et al. (2021) caution that widespread adoption will require standardized frameworks and supportive legal policies. Nonetheless, the convergence of

blockchain technology and digital certification represents a significant shift toward more secure, transparent, and efficient verification processes, which is the primary focus of the DCVS system evaluated in this study.

3. FLOW OF THE PROPOSED SYSTEM



The system involves three main users: Admin (institution), Student, and Verifier. Below is the step-by-step flow of how the system operates:
Step 1: Certificate Generation and Upload (Admin)

- The Admin (e.g., a university) generates a digital certificate (PDF).
- The certificate is uploaded to IPFS.
- IPFS returns a unique hash (CID) for the file.
- This CID (hash) is stored in a smart contract on the Ethereumblockchain, linked with a unique certificate ID or student ID.

Step 2: Certificate Storage

- Only the certificate hash (CID) and metadata like student name, course, etc., are stored on the blockchain to ensure minimal gas costs.
- The actual certificate file remains stored on IPFS, ensuring decentralization and immutability.

Step 3: Certificate Access (Student)

- Students receive their certificate's IPFS link and blockchain ID.
- They can download or share the certificate along with the blockchain-stored verification ID.

Step 4: Verification (Verifier)

- A verifier (e.g., employer) uploads the certificate file or enters the student's ID.
- The system retrieves the stored hash from the smart contract.
- It also calculates the hash of the uploaded file using IPFS.
- If both hashes match, the certificate is valid and authentic.
- If there is a mismatch, the certificate is considered invalid or tampered.

Smart Contract Functions

The core functions of the smart contract include:
issueCertificate(studentId, hash, metadata): Stores certificate hash and associated data
verifyCertificate(studentId, hash): Compares submitted hash with stored hash

getCertificate(studentId): Fetches stored details for display and verification

This methodology ensures:
Immutability: Data stored on the blockchain cannot be changed.
Security: Any tampering with certificates will alter the hash and fail verification.
Decentralization: Eliminates the need for central authorities to verify documents.
Efficiency: Instant verification without requiring manual cross-checking.

4.PROCEDURE

The development of the Blockchain-Based Digital Certificate Verification System is guided by a modular and decentralized architecture that integrates blockchain technology, smart contracts, IPFS, and web-based interfaces to achieve secure, tamper-proof certificate management and verification. The system is built using a combination of React.js for the frontend, Node.js and Express.js for the backend server logic, and Solidity for writing the smart contracts deployed on the Ethereumblockchain. For storing digital certificates, the system uses IPFS (InterPlanetary File System), which provides a decentralized and immutable file storage layer.
During the certificate issuance process, the institution first creates the certificate file and uploads it to IPFS, which returns a unique hash (CID) representing that specific file. This hash, along with relevant certificate metadata such as student ID and course details, is then recorded on the Ethereumblockchain using a smart contract. The smart contract acts as a permanent, tamper-proof registry that maps student identities to their corresponding certificate hashes. By storing only the hash and metadata on-chain and the full certificate off-chain, the system optimizes both security and cost-efficiency.
To verify a certificate, a third party such as an employer can use the system to enter the student ID or upload the certificate. The system then retrieves the stored hash from the blockchain and compares it with the newly generated hash of the provided file using IPFS. If the two hashes match, it confirms the authenticity of the document. This approach eliminates the need for third-party verification and ensures real-time, trustless verification, reducing the chances of fraud and administrative delays. Overall, the methodology leverages blockchain's immutability and decentralization to build a transparent and secure certificate verification framework.

5.Testing

The testing phase of the Blockchain-Based Digital Certificate Verification System was carried out using a local development environment powered by Ganache, which simulates an Ethereumblockchain. The system's frontend was connected to a MetaMask wallet, allowing seamless interaction between the user interface and the smart contracts deployed on the simulated blockchain. Throughout the testing process, various functionalities were validated including certificate issuance, storage on IPFS, hash retrieval, and smart contract interaction.
Unit testing was performed to ensure the correct working of each component—particularly the smart contracts written in Solidity. These were deployed using Truffle Suite, and their functions were tested to validate that only authorized users (e.g., the admin) could issue certificates, and that certificate hashes were accurately stored and retrieved. Additionally, the IPFS integration was tested to confirm that files consistently returned the same hash when unmodified, ensuring integrity.
The verification module was tested by uploading both valid and tampered certificates. In the case of valid certificates, the system accurately retrieved the corresponding hash from the blockchain and confirmed authenticity. For modified or fake certificates, the hash comparison failed, triggering a verification failure alert—demonstrating the system's robustness against forgery.
Overall, the system underwent rigorous testing of both its backend logic and user interface components to ensure a secure, efficient, and user-friendly experience. The successful execution of all test cases confirmed the functional reliability of the certificate issuance and verification process.

6. RESULTS

The Blockchain-Based Digital Certificate Verification System was successfully implemented and tested on a local environment using Ethereum's test network (e.g., Ganache) and deployed via smart contracts written in Solidity. The system supports secure issuance and verification of certificates, leveraging IPFS for file storage and blockchain for hash-based validation.

The following results were observed during testing:

Certificate Issuance:

- Educational institutions can upload certificate files (e.g., PDFs), which are automatically stored on IPFS. A unique content identifier (CID) is generated and stored in a smart contract on the Ethereumblockchain, ensuring immutability.

Verification Process:

- Verifiers can input a certificate ID or upload a certificate file. The system retrieves the stored hash from the blockchain and matches it against the IPFS hash to verify authenticity. The verification process was completed in less than 3 seconds on average.

Security and Tamper Detection:

- Any alteration in the uploaded certificate changes its IPFS hash, which fails verification when compared with the blockchain-stored hash. This ensures tamper-proof validation.

Gas Consumption:

- Smart contract deployment and transactions (certificate hash storage) consumed a moderate amount of gas. Optimization strategies such as storing minimal data (only the hash) were used to reduce costs.

User Interface:

- The frontend built with React.js offered a smooth user experience. Metamask integration enabled seamless interaction with the blockchain.

Scalability Testing:

- The system was tested with 50+ certificate uploads and verification attempts with consistent performance and no failures, indicating good scalability potential for institutional use.
- Overall, the system met its objective of providing a decentralized, transparent, and secure platform for certificate verification, with significant improvements in efficiency and reliability compared to traditional methods.

7. FUTURE WORK

While the current implementation of the blockchain-based digital certificate verification system demonstrates the core functionality of secure issuance and verification, there are several areas in which the system can be further enhanced to improve scalability, usability, and adoption.

1. Multi-Institution Support:

The system can be expanded to support multiple educational institutions through role-based access and a modular smart contract structure. This would allow universities and training centers to use a common platform while maintaining control over their own certificate data.

2. QR Code Integration:

Certificates can include a QR code that links directly to their IPFS hash or verification page. This would enable quick and convenient scanning and verification by employers or institutions using mobile devices.

3. Mobile Application:

A mobile app version of the system could increase accessibility and allow students and verifiers to upload or verify certificates on the go. This would also promote wider usage in regions where mobile devices are more prevalent than computers.

4. Digital Identity Integration:

The platform could be integrated with decentralized identity (DID) systems to create a complete digital identity solution, linking certificates to verified student profiles.

5. AI-Based Fraud Detection:

Machine learning models could be added to detect suspicious or potentially fake uploads and prevent misuse of the platform.

8. CONCLUSION

The increasing prevalence of certificate fraud and the inefficiencies of traditional verification methods underscore the need for a secure, decentralized solution. This paper presents a Blockchain-Based Digital Certificate Verification System that leverages the immutability and transparency of blockchain along with the distributed storage capabilities of IPFS to provide a tamper-proof mechanism for issuing and verifying digital certificates.
By utilizing Ethereum smart contracts, this system ensures that each certificate's authenticity can be independently validated without relying on a central authority. The integration with IPFS allows certificates to be stored in a decentralized manner, with their hashes permanently recorded on the

blockchain, making any form of manipulation instantly detectable.The proposed system demonstrates how emerging technologies can be effectively combined to solve real-world problems in education, employment, and beyond. It not only enhances trust in digital credentials but also reduces verification time and operational overhead. Though challenges such as gas costs and user accessibility remain, the system lays a solid foundation for future improvements and broader adoption.

In conclusion, blockchain offers a transformative approach to digital certificate management, and this project provides a practical implementation that can be further developed and scaled to meet institutional and industry needs.

REFERENCES:

1. J. Grech and A. Camilleri, "Blockchain in Education," European Commission Joint Research Centre, 2017. [Online]. Available: https://op.europa.eu/s/pxy6
2. J. Sharples and R. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward," Knowledge Media Institute, The Open University, 2016.
3. MIT Media Lab, "Blockcerts: The Open Standard for Blockchain Certificates," 2016. [Online]. Available: https://www.blockcerts.org
4. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
5. "Ethereum Whitepaper," Ethereum Foundation. [Online]. Available: https://ethereum.org/en/whitepaper/
6. Protocol Labs, "IPFS - InterPlanetary File System," [Online]. Available: https://ipfs.tech/
7. AmritBhusal, "Blockchain Based Digital Certificate Verification System," GitHub Repository, 2022. [Online]. Available: https://github.com/AmritBhusal/DCVS
8. A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, "Bitcoin and Cryptocurrency Technologies," Princeton University Press, 2016.