AVE Trends in Intelligent Computing Systems

Enhancing Certificate Authentication Through a Transparent Blockchain Enabled Verification System

B. J. Sruthi[1,*], J. Princy Jeniffer[2], K. Sri Harshita[3], M. Rehena Sulthana[4], C. Christina Angelin[5]

[1,2,3]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
[4]School of Information Technology and Engineering, Melbourne Institute of Technology, Melbourne, Victoria, Australia.
[5]Department of Mathematics, Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.
sb6770@srmist.edu.in[1], pj9534@srmist.edu.in[2], sk8316@srmist.edu.in[3], rsulthana@academic.mit.edu.au[4], christeenaangelin@gmail.com[5]

*Corresponding author

Abstract: Traditional systems of verification and validation of certificates are prone to misuse, misplacement and inefficiency. These systems require manual verification and are time-consuming and error-prone. The article presents a Blockchain-Based Certificate Validation System that guarantees Security, transparency and permanency in the validation of certificates. Using a smart contract and a decentralised store, certificates are issued and stored securely in a tamper-proof ledger, eliminating the need for third-party dependence and reducing the time taken to verify. The system utilises Ethereum for smart contracts, IPFS for decentralised storage, and cryptographic hashing for data integrity. Gas fee optimisation techniques are used for minimising costs and ensuring secure and verifiable certificate issuance while improving transaction efficiency. A combination of on-chain and off-chain storage is used to reduce blockchain congestion and enhance scalability. By achieving a substantial improvement in cost efficiency, reliability and availability, this approach provides an affordable and secure solution for academic institutions, employers and government departments. Combining blockchain technology with digital credential verification improves trust among all the stakeholders and creates a secure, unchangeable, and scalable basis for modern digital certification.

Keywords: Blockchain Technology; Certificate Verification; Smart Contracts; Ethereum and Cryptographic Hashing; Secure Credentialing; Trustless Verification; Traditional Systems; Digital Transformation.

Cite as: B. J. Sruthi, J. P. Jeniffer, K. S. Harshita, M. R. Sulthana, and C. C. Angelin, "Enhancing Certificate Authentication Through a Transparent Blockchain Enabled Verification System," *AVE Trends in Intelligent Computing Systems*, vol. 2, no. 1, pp. 15–26, 2025.

Journal Homepage: https://www.avepubs.com/user/journals/details/ATICS

Received on: 13/07/2024, **Revised on:** 01/10/2024, **Accepted on:** 20/11/2024, **Published on:** 05/03/2025

DOI: https://doi.org/10.64091/ATICS.2025.000102

1. Introduction

Today, in the time of rapid adoption of digital transformation in industries, the credibility of safe and reliable credential verification systems has never been more significant. Educational institutions are increasingly forced to use traditional means of verification with the rising incidence of fake degrees, forged resumes and credential fraud. Traditional verification is a multi-staged process primarily based on third-party agencies, which means delays, high costs, and a high sensitivity to misrepresentation. To overcome these endless difficulties, a faster, tamper-proof system is required, permitting proof-of-accreditation and professional certification without relying on centralised authorities. Among the many reasons to believe that

blockchain will be a help is its decentralised, transparent and immutable features as an architectural foundation. As a decentralised ledger, blockchain keeps a record of data once logged in; this cannot be changed or deleted for a single node, so it is ideal for issuing and verifying certificates.

Academic institutions can dispense credentials as distinct digital assets, associated with a cryptographic hash via smart contracts and thereby certify their genuineness, as well as shielding them from duplication, but also from being forged. Besides that, when QR codes are made and tied to the blockchain, they can be easily verified by employers and other institutions as they allow the credentials to be instantly verified without requiring an intermediary. Besides its fundamental functionality, the integration of decentralised storage solutions like the InterPlanetary File System (IPFS) deepens the system security and resilience, in part due to the adoption of blockchain ASICs today. Since traditional centralised databases can be hacked and tampered with, IPFS provides the distributed, secure storage of credential-related data (but not license or permit information), which ensures that its availability and integrity are maintained.

2. Literature Review

Several studies have explored blockchain technology for secure certificate verification, addressing challenges such as fraud prevention, centralisation, and high verification costs. Aparna and Kesavamoorthy [1] proposed a blockchain-based decentralised model that integrates certificate authentication and issuer validation within a single platform. Their approach uses an Ethereum-like transparent blockchain, ensuring tamper-proof verification while optimising energy consumption and transaction costs. Experimental results indicate that the proposed system outperforms existing methods in terms of cost-efficiency and Security. The application of blockchain technology in academic certificate verification has gained significant attention due to its potential to address fraud, inefficiency, and reliance on central authorities.

Rustemi et al. [2] conducted a systematic literature review on blockchain-based systems for academic certificate verification, analysing existing research on immutable digital credentials and their impact on the education sector. Their study highlights how blockchain can enhance traditional verification methods by making them faster, more reliable, and decentralised. Despite advancements, they note that research in this domain is still in its development phase, requiring further exploration for large-scale adoption. Blockchain-based certificate verification systems aim to provide tamper-proof, decentralised, and cost-efficient authentication mechanisms. Leguizamo et al. [4] propose an integrated blockchain-based system that ensures both certificate authentication and issuer validation within a single platform.

The study leverages the Ethereum blockchain and hash function mapping to enhance Security and optimise search efficiency. Their experimental evaluation demonstrates that the proposed system minimises gas consumption while reducing search time for certificate validation. Comparative analysis with existing methods confirms that this approach offers lower costs and improved performance, making it a promising solution for large-scale adoption. With the rise of digital certificate forgery, blockchain technology has emerged as a promising solution for secure verification. Tey et al. [5] propose a blockchain-based framework that leverages smart contracts on the Ethereum network for verifying digital document signing certificates. Their approach ensures that certificates are securely stored, accessed, and validated through predefined smart contract conditions. Security testing using Slither and Solhint confirms the system's resilience against vulnerabilities. The study demonstrates that blockchain-based smart contracts can effectively prevent certificate forgery, making them applicable to broader information system developments.

Traditional document verification methods are prone to fraud and inefficiencies. Louis and Catur Candra [6] propose EduDocs, a blockchain-based system that ensures secure and tamper-proof authentication using cryptographic hashing and smart contracts. Their approach eliminates intermediaries, enhancing Security and transparency. Experimental results confirm its superiority over centralised solutions, making blockchain a viable alternative for document verification. This paper, published by Ankit et al. [7], proposes a blockchain-based digital certificate verification system to prevent counterfeiting and unauthorised modifications. Their approach leverages tamper-proof data storage and hash functions to ensure secure, immutable, and authenticated certificates. A transparent network enables peer-approved digital certification, enhancing trust and eliminating centralised control. Additionally, smart contracts automate verification processes, ensuring data integrity and Security. The study highlights blockchain's potential to revolutionise digital certification while addressing security concerns.

Goswami et al. [8] propose a blockchain-based e-certification framework to streamline academic certificate validation. Their approach automates certificate issuance and verification, utilising cryptographic hashing and QR codes to ensure authenticity and Security. The system enhances ownership control, transparency, and efficiency, significantly reducing manual effort and paper usage. Empirical results demonstrate superior performance compared to traditional verification methods, positioning blockchain as a sustainable and efficient alternative. Pradeep et al. [3] propose a blockchain-based certification system to address the growing challenge of fake academic credentials. Their model ensures secure, immutable verification of academic records, allowing students to access credentials affordably and enabling employers to verify degrees efficiently. The

decentralised nature of blockchain ensures data integrity, preventing unauthorised alterations. This solution reduces the time and cost of verification, making it a reliable alternative to traditional methods.

The paper by Usha and Thenmozhi [9] explores the idea of utilising blockchain-based frameworks to detect fake certificates and verify academic credentials. It examines various hashing techniques, cryptographic methods, and smart contracts employed in blockchain authentication. The study discusses the strengths and limitations of existing verification systems while emphasising the importance of secure, decentralised, and efficient solutions. Additionally, it provides insights into blockchain advancements aimed at preventing certificate fraud. Obaid et al. [10] investigate the use of blockchain technology for secure digital degree issuance and verification, aiming to mitigate certificate forgery. Their proposed system utilises a decentralised ledger to enhance transparency, Security, and auditability in academic credential verification. The study highlights how immutable blockchain records and IPFS storage ensure data integrity while integrating Aadhar-based authentication for enhanced reliability. By utilising blockchain's distributed and tamper-proof nature, the research demonstrates a secure and efficient alternative to traditional certificate verification methods.

2.1. Proposed Architecture

Figure 1 describes a Certificate Verification System on the Blockchain that provides a secure, transparent, and decentralised platform for issuing and verifying academic and professional credentials. By leveraging blockchain technology, it eliminates forgery, reduces verification time, and ensures tamper-proof certificates. Unlike traditional systems requiring third-party agencies, this solution allows institutions to issue certificates directly on the blockchain, making them immutable and instantly verifiable by all stakeholders. The system includes a web server as the main user interface, with web and mobile apps for accessing, sharing, and verifying credentials. Institutions can issue certificates, students manage records, and employers verify them in real time. The backend API handles certificate issuance, verification, and blockchain interactions while securely managing user data in a database.

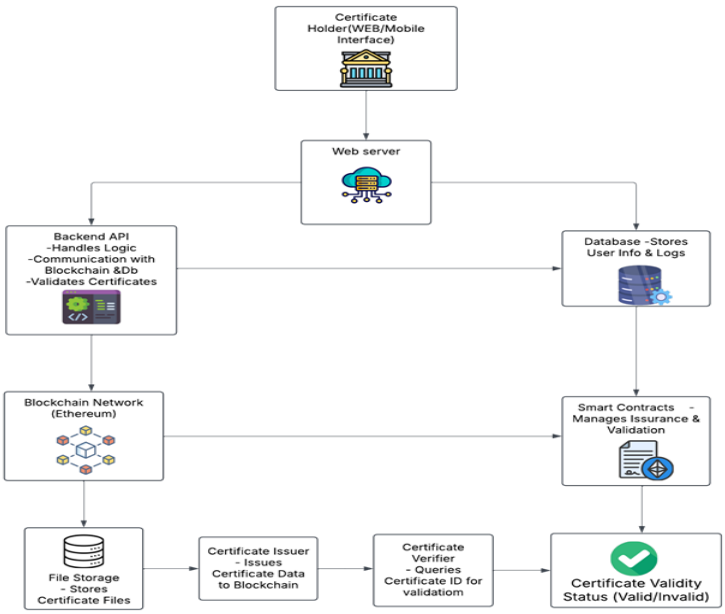

Figure 1: Blockchain certificate verification process flow

Each certificate is assigned a unique cryptographic hash stored on the Ethereum blockchain, preventing unauthorised alterations. The actual certificate files are securely stored on IPFS, linked to the blockchain via unique hashes. Smart contracts ensure only authorised issuers can generate certificates, and verifiers can instantly authenticate them via certificate IDs or QR codes. This scalable, tamper-proof system effectively reduces verification costs, prevents fraud, and enhances trust among students, institutions, and employers. The proposed architecture for a blockchain-based digital certificate verification system aims to create a safe, transparent, and decentralised platform for issuing and verifying academic and professional qualifications.

Traditional verification procedures rely on centralised authorities and human authentication, which are prone to inefficiencies, forgery, and delays. With the application of blockchain technology, this system ensures that once a certificate is created, it

cannot be changed and is tamper-proof, eliminating any unauthorised changes. The system comprises a couple of key components, including a blockchain network, smart contracts, decentralised storage, a web-based user interface, and an authentication mechanism for secure transactions. They work together to provide an end-to-end solution for the issuing institutions, the students managing their credentials, and the employers verifying the legitimacy of qualifications. Unlike the conventional system based on third-party verification bureaus, this decentralised approach eliminates mediators, reducing verification time and expense and enhancing Security and trust in the credentialing process.

The blockchain network is at the centre of this architecture and serves as a public ledger where certificate records are stored. Institutions utilise smart contracts to issue certificates as digital assets on the Ethereum blockchain. A unique cryptographic hash is assigned to every certificate, ensuring that its integrity is maintained over its lifetime. These smart contracts regulate the issue, storage, and recovery of certificates so that authorised institutions can create verifiable digital credentials which can be viewed by students and verified by employers. Furthermore, to make efficient use of storage, the system incorporates the InterPlanetary File System (IPFS). This open-source, decentralised storage protocol securely hosts real certificate files while connecting their respective hashes to the blockchain. This two-layered system guarantees that even when a certificate document is kept off-site, its authenticity can always be traced to an unchangeable blockchain record. In addition, every certificate issued is linked to a QR code, which allows for immediate verification by simply scanning the code or querying the blockchain for the credential details stored.

This architecture provides various security improvements to avert fraudulent activity and unauthorised amendments. Because records on blockchain are immutable, once a certificate is issued, it can never be deleted or modified, and thus, data integrity is provided. The decentralised system structure eradicates the threat of single points of failure, rendering it robust against cyberattacks and data breaches. Additionally, since certificate verification is done on the blockchain itself, no middlemen are necessary, lowering costs and processing time. Also integrated into the architecture are considerations for privacy so that students and professionals have control over who has access to their credentials, thus ensuring that sensitive information is not leaked unauthorised. By overcoming the shortcomings of conventional verification processes, this suggested blockchain-based system offers a scalable, effective, and fraud-proof mechanism for managing educational and professional credentials, thereby leading to a more transparent and reliable environment in academic and employment markets.

The frontend of the system is developed in React.js, and it is user-friendly for institutions, students, and employers. Institutions can upload and distribute digital certificates using a basic web interface. Students can see and control their certificates as a digital wallet. Employers can authenticate a candidate's certificate by scanning a QR code or searching for it in the verification portal. The backend, coded in Node.js and Express.js, bridges the frontend to the blockchain and the decentralised storage. Web3.js or Ethers.js facilitates the interaction with smart contracts for issuing, downloading, and verifying certificates. The system also adds Security by keeping only authorised institutions in charge of issuing or revising certificates, while students maintain sole authority over issuing their credentials.

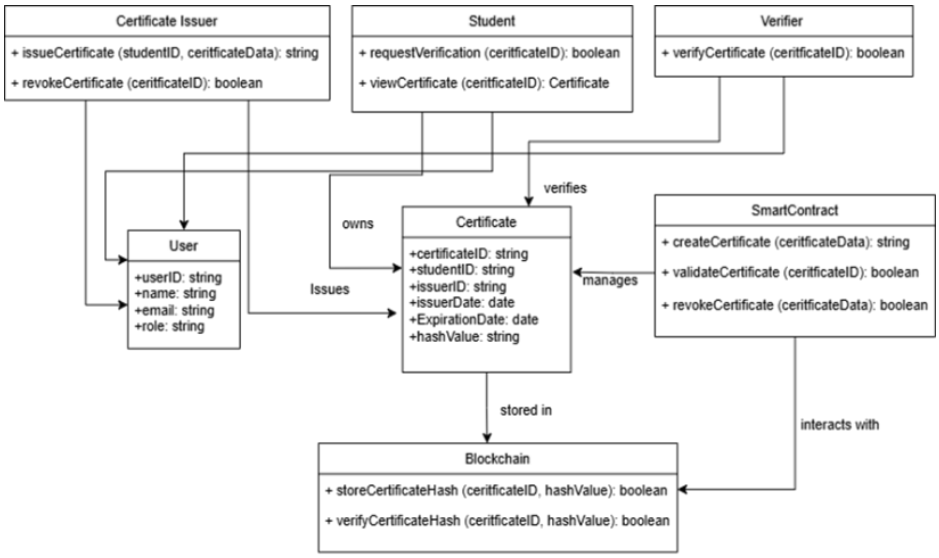

Figure 2: Functional overview of certificate verification

Figure 2 depicts the architecture of the blockchain-based certificate verification system, with important entities and their relationships. It consists of classes such as User, CertificateIssuer, Student, Verifier, Certificate, Blockchain, and SmartContract.

CertificateIssuers create and revoke certificates, while Students own and request Verification. Verifiers verify certificates by comparing blockchain-stored hashes, which is secure and transparent. The SmartContract handles certificate creation, validation, and revocation, interacting with the Blockchain to store unalterable certificate information. This process ensures a decentralised, tamper-proof, and secure way to validate digital credentials.

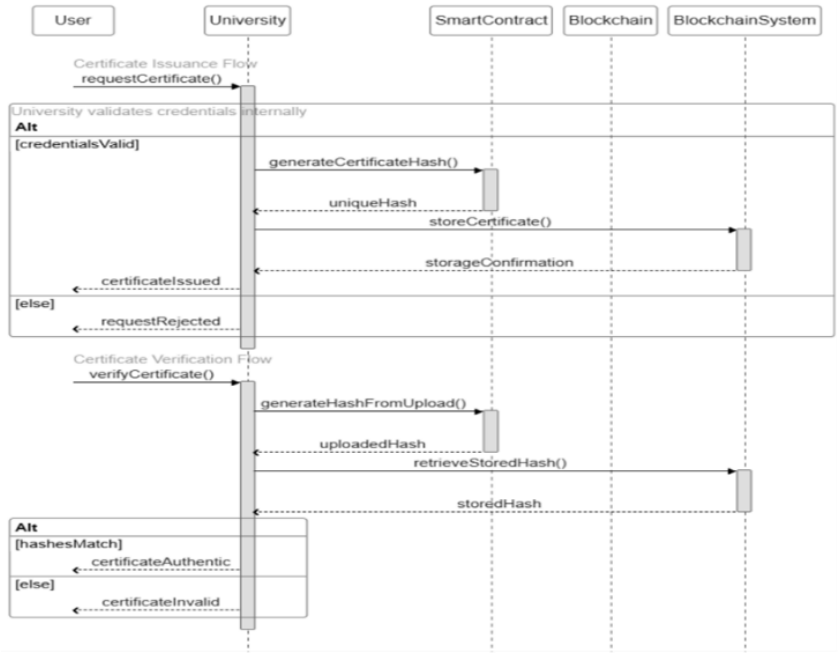

Figure 3: Interaction flow for certificate issuance and verification

Figure 3 presents the stepwise process of issuing, storing, and authenticating academic certificates securely and in an unalterable way. The procedure starts with a request for a certificate from a user (institution or student), which is authenticated by the university using student credentials. In case of approval, a smart contract creates a hash of the certificate, which is safely stored on a blockchain and IPFS (InterPlanetary File System). Upon receiving a verification request from an employer or institution, the system retrieves the stored certificate hash from the blockchain and verifies it against the uploaded certificate. If the hashes are identical, then the certificate is confirmed to be authentic; else, it is invalid.

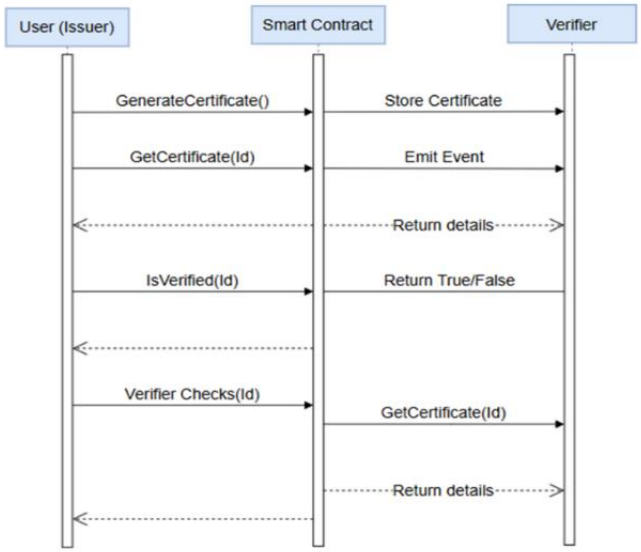

Figure 4: Smart contract interaction for certificate management

Figure 4 sequence diagram depicts the main interactions in the Certificate Verification System through a blockchain-based smart contract. Initially, the User (Issuer) calls generate Cert (ID), which saves the certificate on the blockchain and emits an event to confirm its creation. Then, the Verifier (for example, an employer or university) or any user can retrieve the certificate details via the getCert (ID) method. To verify the certificate's authenticity, they can call isVerified (ID), which checks the certificate's existence and returns True or False. If the Verifier needs more details, he can ask for a certificate directly, ensuring secure and straightforward validation.

2.2. Execution of Key Functions

2.2.1. Certificate Issuance Function

The core system functionality of our blockchain-based certification system is to issue digital certificates securely and transparently. The Issue Certificate method ensures that certificates are uniquely assigned to individuals, preventing duplication or unauthorised modification. Only authorised entities, such as educational institutions or organisations, can issue certificates. To ensure data security, each certificate is linked to a hashed Aadhar number, which acts as a unique identifier without exposing sensitive personal information. When a certificate is issued, it is permanently stored on the blockchain, making it immutable and verifiable at any time.

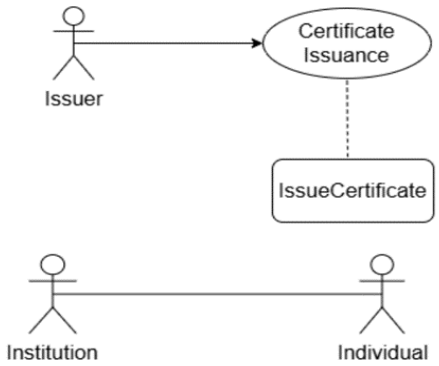

Figure 5: Descriptive diagram of the issued certificate

The implementation of the smart contract follows best practices in Solidity. Figure 5 depicts the usage mapping structures to link the hashed Aadhar numbers to their corresponding certificate hashes. The certificate issuance is restricted to the owner of the contract. Thus, only authorised personnel can add a new certificate. This approach decreases the risk of fraudulent certificates and ensures the integrity of the issued credentials.

2.2.2. Sample Transaction for Certificate Issuance

Figure 6 describes that once a certificate is issued, an Ethereum transaction is generated and recorded on the blockchain. The transaction confirms that the certificate issuance process was completed on the Ethereum network. The transaction hash is a unique reference that can be used to verify the issuance record. The gas used is the computational cost of the transaction and is crucial for optimising the smart contract efficiency. The execution time is the time taken for the transaction to be processed, demonstrating system responsiveness.

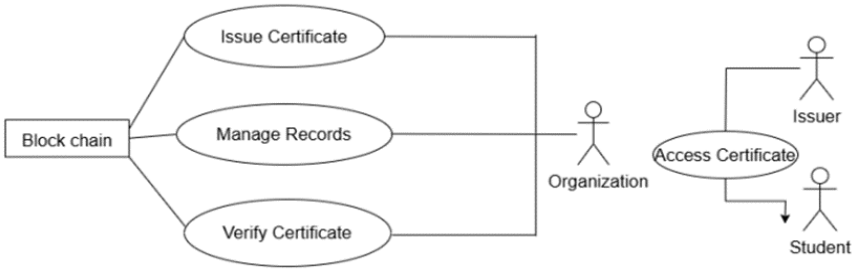

Figure 6: Transaction for issuance

2.2.3. Security and Privacy Considerations

As shown in Figure 7, Security and privacy are the foundations of our certification system. By implementing blockchain technology, we ensure that certificates are secure and unchangeable, thereby eliminating the possibility of counterfeiting. Hashing techniques protect sensitive personal data by storing Aadhar numbers, allowing for unique identification. Furthermore, blockchain's immutability ensures that certificates cannot be changed or deleted, which guarantees the veracity of academic and professional certificates. To boost Security, we support smart contract event logging in our implementation. This gives you the ability to track when certificates are issued in real time, enabling you to catch anomalies and prevent unauthorised changes. Further, we will add a mechanism to provide a multi-signature approval in future versions, and only after passing this mechanism, the certificate will be issued.

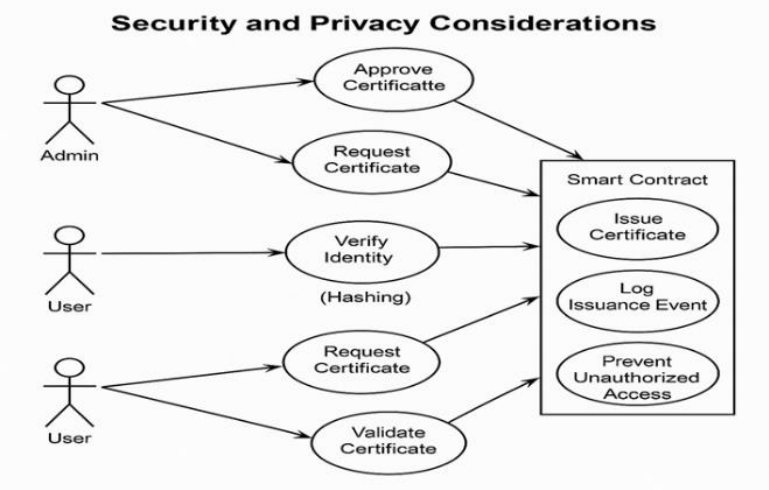

Figure 7: Use case diagram for security functions

2.2.4. Comparison with Traditional Certification Systems

The blockchain-based certification system offers a reliable alternative to the traditional certificate issuance, which is vulnerable to fraud, loss or delay. In a paper-based system, certificates can be forged or lost, and verification requires a manual process, which is time-consuming. Digital centralised certificate systems are faster but can be subject to data breaches and unauthorised access.

Our blockchain-based solution offers a decentralised and transparent way to store certificates on an immutable ledger. It allows for real-time verification, significantly reducing processing time. However, it has some limitations, such as high gas fees on public Ethereum networks and the complexity of integrating blockchain with existing institutional frameworks. Future improvements may include Layer 2 scaling solutions to reduce transaction costs and integration with IPFS to store certificates in a decentralised and cost-efficient way.

2.2.5. Challenges and Limitations

Throughout the project development and implementation, the team faced several challenges. The first challenge was optimising gas, as Ethereum transactions are not cheap. It was necessary to carefully structure the deployment of smart contracts and the execution of some functions, like issuing certificates, to minimise gas fees. The second challenge was the storage limitations in Solidity, which made it impossible to store large certificate files on-chain directly. This required hashing techniques to be employed.

Moreover, another key challenge was the scalability. As the number of issued certificates grows, it is necessary to maintain the efficiency of blockchain storage and retrieval. One possible solution is to integrate off-chain storage mechanisms like IPFS or Arweave, allowing the blockchain to store only essential metadata, while keeping certificate files decentralised and accessible. In addition to this, user adoption remains a limitation, as many institutions are still unfamiliar with blockchain technology. Therefore, providing a user-friendly interface and educational resources will be essential to encourage widespread adoption.

2.3. Solidity Program

2.3.1. Certificate Verification.sol

The Solidity smart contract is called certification. It is a way to store and verify digital certificates securely using the blockchain. The contract describes a Certificate structure (Figure 8). Such a contract ensures that the certificate is real and cannot be changed after it is signed. This is perfect for blockchain-based systems of certificate verification (Figure 9).

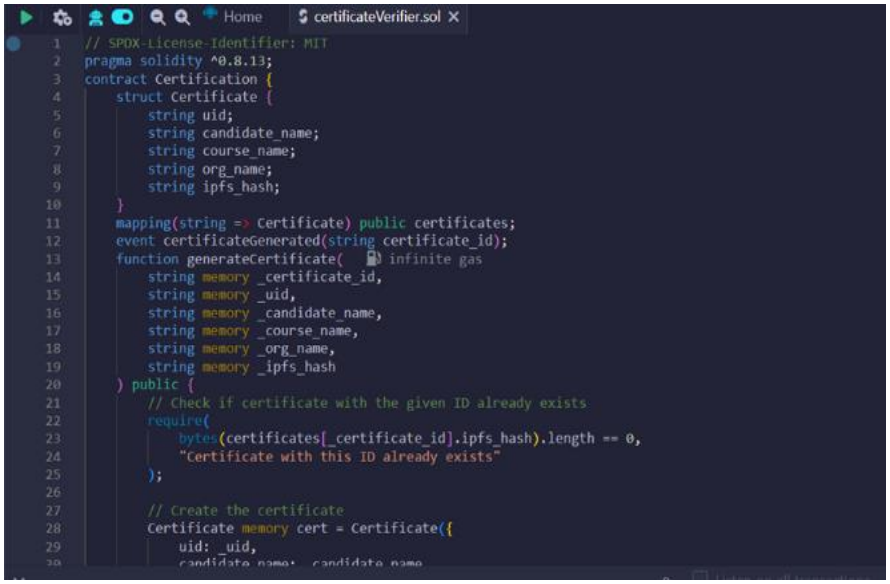

Figure 8: Certificate structure and generation function definition

This structure contains data such as the candidate's name, the course name, the issuing organisation, and a hash on IPFS that stores the certificate. The certificate ID saves all certificates. The function generates Certificate checks that the new certificate has a unique certificate ID before saving it.

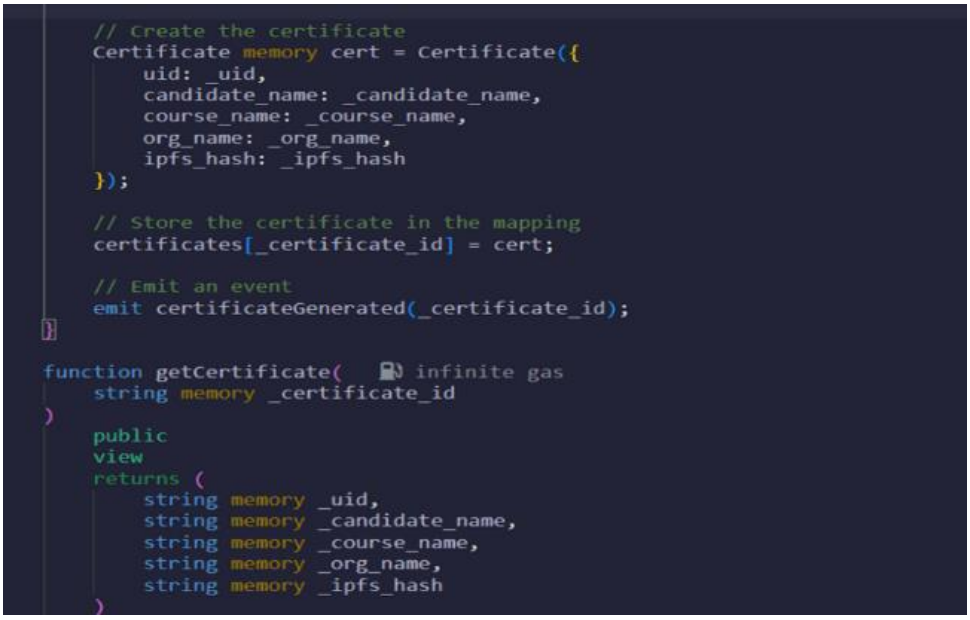

Figure 9: Certificate creation, storage, and event emission

The get Certificate function allows you to read the certificate (Figure 10). The function verifies whether the certificate exists. It does this by checking the hash on IPFS. The event certificate generated keeps track of creating a new certificate.

```
    {
        Certificate memory cert = certificates[_certificate_id];
        // Check if the certificate with the given ID exists
        require(
            bytes(certificates[_certificate_id].ipfs_hash).length != 0,
            "Certificate with this ID does not exist"
        );

        // Return the values from the certificate
        return (
            cert.uid,
            cert.candidate_name,
            cert.course_name,
            cert.org_name,
            cert.ipfs_hash
        );
    }
    function isVerified(    infinite gas
        string memory _certificate_id
    ) public view returns (bool) {
        return bytes(certificates[_certificate_id].ipfs_hash).length != 0;
    }
}
```

Figure 10: Certificate retrieval and verification functions

3. Result and Discussion

The bar chart Figure 11 compares three types of systems — Blockchain, Centralised Database, and Paper-Based — across five factors: Security, transparency, efficiency, scalability, and cost, as shown in Table 1. According to the chart, Blockchain outperforms the other two systems in Security and transparency due to its decentralised and immutable nature.

Table 1: Comparison of data storage methods

Attribute	Blockchain	Centralized Database	Paper-Based
Security	9	5	2
Transparency	9	2	1
Efficiency	9	5	2
Scalability	9	5	2
Cost	5	6	6

The Centralised Database is also secure, more efficient and scalable than the paper-based system. However, the paper-based system is the cheapest, as data is manually verified and processed. Lastly, while Blockchain is cheaper than the paper-based system, it is more expensive than the Centralised Database due to its complexity. In conclusion, Blockchain is the most secure and transparent, while the paper-based system is the least efficient and most expensive.

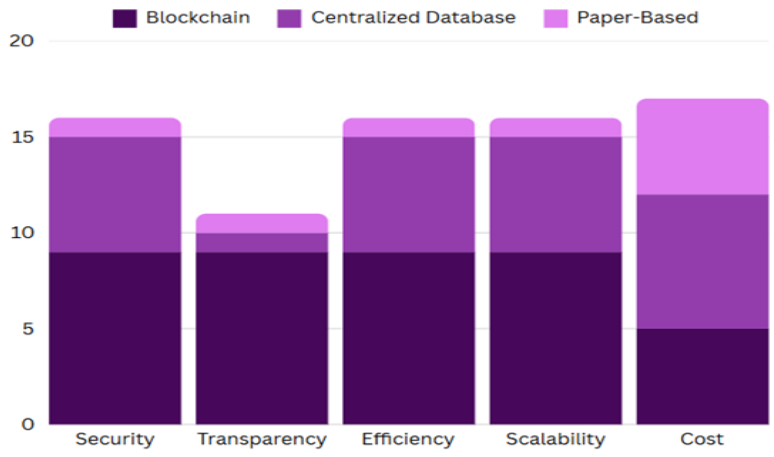

Figure 11: Credential verification comparison graph

Figure 12 illustrates the distribution of various certificate verification methods, as detailed in Table 2. It shows that blockchain-based verification is the most adopted at 31%, due to its Security, decentralisation, and immutability. Public Key Infrastructure (PKI) follows at 24.1%, valued for its reliability in digital security applications.

Table 2: Various certificate system verification methods

Method	Percentage (%)
Blockchain	31.0
Public Key Infrastructure	24.1
DHT systems	20.7
Centralized Database	20.7
Paper-Based	3.4

Distributed Hash Table (DHT) systems and centralised databases account for 20.7%, reflecting their significance in data storage and verification. Paper-based systems have the lowest adoption at 3.4%, a trend that is decreasing as digital solutions become more prevalent.

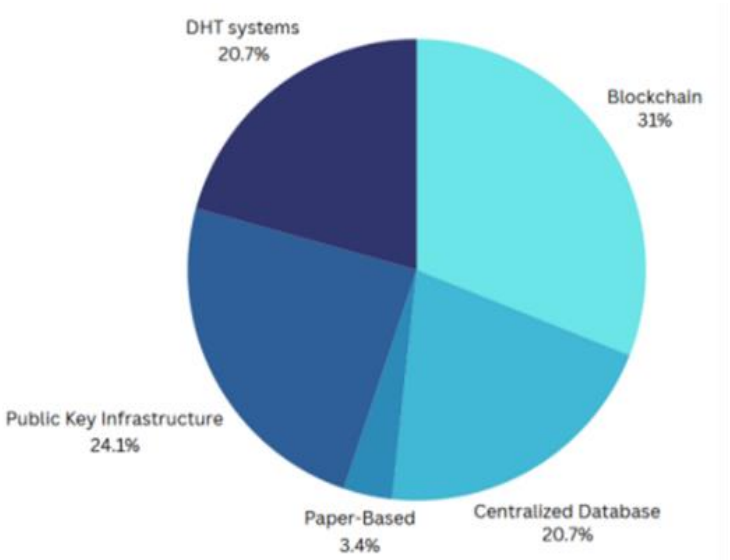

Figure 12: Credential verification distribution graph

Table 3 gives a comparative indication of various digital certificate verification methods as regards their accuracy, verification time, scalability and certificate integrity. The Centralised Database System offers high scalability with a quick verification time of 1 second, but it has lower accuracy (95%) and lower certificate integrity (98%) due to weaknesses in Security.

Table 3: Detailed results and comparison to other works

Approach	Accuracy	Verification Time (s)	Scalability	Certificate Integrity
Centralised Database System	95%	1	High	98%
Public Key Infrastructure (PKI)	97%	3	Medium	99%
Blockchain-Based System with QR Codes	98%	2	Medium	100%
Blockchain (Proposed)	99%	2	High	100%

Public Key Infrastructure (PKI) increases certificate integrity (99%) but decreases the verification speed to 3 seconds, whereas the scalability went down to 97% for accuracy. The Blockchain-Based System with QR Codes boosts accuracy up to 98% and guarantees absolute certificate integrity (100%), coupled with an average verification time of 2 seconds and medium scalability. Proposed Blockchain System enhances accuracy (99%), and certificate integrity (100%); has secured, decentralised verification; low verification time (2 seconds) and high scalability as well. This study states that blockchain-based solutions provide higher Security and trustworthiness than traditional methods and are well-suited for digital certificate verification (Figure 13).

The above is an unsuccessful verification process. When a forged or invalid certificate ID or file is presented, the system checks it against other blockchain records and fails to get a match. The system presents an alert, stating that the certificate is fake, tampered with, or is not present in the system. It does not allow fraud and ensures that only legitimate credentials are validated.

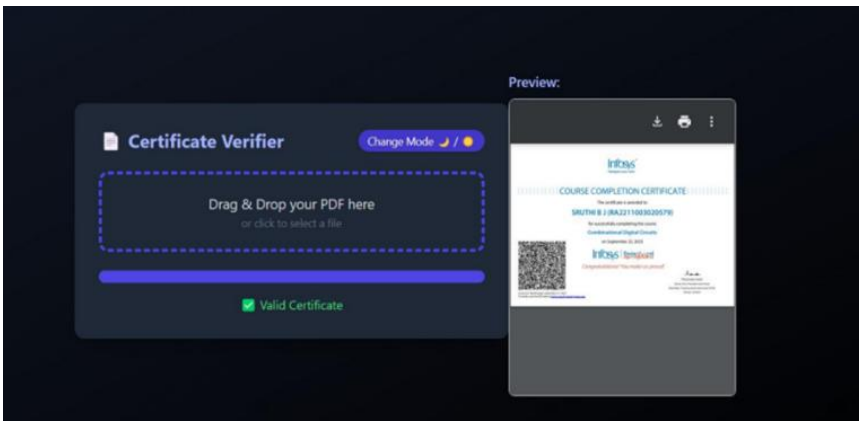

Figure 13: Verification result for a valid certificate

The following screenshot demonstrates a successful verification result via the blockchain frontend interface. Upon input of a correct certificate ID, the system reads the corresponding hash from the blockchain and compares it with the uploaded document. The message is presented that the certificate is authentic and tamper-free. This instils trust and transparency in the verification process (Figure 14).

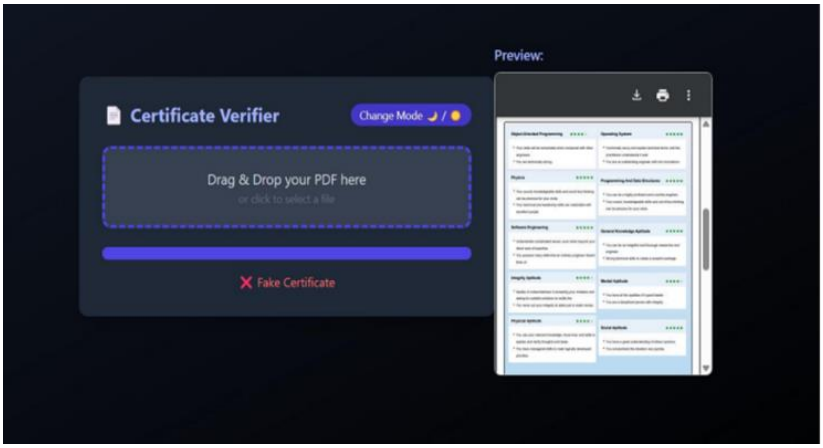

Figure 14: Verification result for a fake certificate

4. Conclusion

The proposed blockchain-based digital certificate verification system provides a decentralised, secure, and tamper-proof process for issuing and authenticating academic diplomas. Traditional methods are lengthy, costly, and susceptible to counterfeiting, whereas blockchain provides immutability and prevention against unauthorised manipulation. By utilising smart contracts on the Ethereum blockchain and decentralised storage on IPFS, the system eliminates the need for third-party verification bureaus, reducing processing time and ensuring data integrity while saving costs. A React. js-based web interface and a backend powered by Node.js and Express.js enable effortless interaction among institutions, students, and employers. Smart contracts enable automatic recovery and issuance of certificates, with QR code-based verification providing an added layer of convenience.

The decentralised design rules out single points of failure, offering enhanced Security and protection from cyberattacks, with privacy attributes that allow users to control who can access their credentials. This system not only builds confidence and trust in academic and professional credential management but also provides an economical, cost-saving, fraud-proof, and scalable solution. By eliminating inefficiencies and security problems with traditional credentialing, it catalyses a more efficient, reliable, and future-proof digital certification ecosystem.

Acknowledgement: The authors sincerely thank all for their guidance and encouragement, which greatly contributed to the successful completion of this work.

Data Availability Statement: The study utilises a dataset related to Enhancing Certificate Authentication Through a Transparent Blockchain Enabled Verification System. The dataset is available upon reasonable request to the corresponding author.

Funding Statement: This research and manuscript preparation received no financial support or external funding from any organisation or agency.

Conflicts of Interest Statement: The authors declare that there are no conflicts of interest associated with this study. All sources of information have been appropriately cited and referenced.

Ethics and Consent Statement: Informed consent was obtained from all participating individuals and the involved organisation during the data collection process. Research standards were duly secured, ethical approval and participant consent.

References

1. N. Aparna and R. Kesavamoorthy, "Exploring Blockchain Solutions for Combating Fake Certificates," *2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, Trichy, India, 2023.
2. A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," *IEEE Access*, vol. 11, no. 6, pp. 64679–64696, 2023.
3. C. D. Pradeep, M. Ashislh, R. Aishwarya, and R. Yogitha, "A Blockchain Application for the Verification of Academic Information and Scalable Certification," *2023 7th International Conference on Computing Methodologies and Communication (ICCMC),* Erode, India, 2023.
4. C. P. Leguizamo, S. Kato, K. Kirai, and K. Mori, "Autonomous decentralized database system for assurance in heterogeneous e-business," *25th Annual International Computer Software and Applications Conference*. COMPSAC 2001, Chicago, Illinois, United States of America, 2001.
5. F. C. Tey, N. M. Ahmad, and S. F. A. Razak, "Blockchain-based Mutual Authentication Model for Customer Services," *2023 11th International Conference on Information and Communication Technology (ICoICT),* Melaka, Malaysia, 2023.
6. F. I. Louis and M. Z. Catur Candra, "Blockchain-Based Public Key Infrastructure Using Smart Contracts," *2024 IEEE International Conference on Data and Software Engineering (ICoDSE)*, Gorontalo, Indonesia, 2024.
7. K. C. Ankit, D. Bhandari, R. Priyadarshini, and P. K. Meher, "Detection of Fake Physical Certificates using a Blockchain-Based Certificate Verification and Issuer Validation System," *2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS),* Pune, India, 2024.
8. K. Goswami, D. Vaithiyanathan, P. Verma, and B. Kaur, "Document verification using Blockchain," *2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE)*, Shivamogga, India, 2024.
9. K. Usha and T. Thenmozhi, "Blockchain-Based Secured and Privacy Protected Academic Certificate Management System," *2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)*, New Raipur, India, 2023.
10. M. Obaid, A. Abumwais, R. Hodrob, and S. Odeh, "A Blockchain-Based Framework for Efficient and Secure E-Certification Sharing and Verification," *2024 25th International Arab Conference on Information Technology (ACIT)*, Zarqa, Jordan, 2024.