International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

A Secure Blockchain-Based Framework for Academic Certificate Authentication and Validation

Sarwesh kumar, Keshav Kumar
Department of Computer Science And Engineering, Sharda University, Greater Noida, UP

Abstract -- With the increase in the adoption of digital education and online certifications, there is a remarkable need for certificate verification systems that are secure and reliable. Certificate issuance and validation are traditionally conducted through a manual process relying on centralized databases that is easily forged, manipulated, and fails in the occurrence of an accidental data loss. A big cause of concern for educational institutions, employers and government agencies is fake certificates. To alleviate such problems, a tamper-proof and distributed certificate verification mechanism is proposed on the basis of block chain technology. The blockchain technology offers a decentralized and unchangeable ledger, like cannot change the data once stored in that ledger. The new system stores the verified certificates into a blockchain network securely after being issued by institutions. It assigns a unique cryptographic hash value for each certificate to ensure its authenticity and integrity.

Keywords - Blockchain, technology, verification, decentralized, databases, authenticity

I. INTRODUCTION

Each year, millions of certificates are handed over to students from academic programs by universities in the current digital world. Certificates are proof of quality, and are used for higher education, job opportunities, and professional status. Certificates have historically been issued in physical form and recorded in centralized databases controlled by institutions. But, this conventional system faced number of challenges like forgery of certificates, loss of documents, slow verification process and lack of transparency.

Credential verification is not only time-consuming; it is also inefficient as it relies on contacting the issuing institution to verify a certificate. In a lot of cases, these organizations must depend on 3rd party verification services leading to an increase in cost and processing time. Additionally, centralized databases are susceptible to cyber attacks, data tampering, and unauthorized alterations.

Blockchain has come up as a possible solution to deal with this issue. It is a kind of distributed ledger technology where information is stored on multiple nodes in a decentralised network. Every block of the chain will have the cryptographic hash of the previous one, so nobody can tamper anything's that stored in it. This guarantees data integrity as well as security. This may include storing them in a blockchain, where institutions can store certificates immutably. Once certificate is uploaded into the blockchain network; it will be immutable and can not be manipulated with out consensus of the networks. Their proposed system also includes QR code technology for the certificate verification process.

II. PROBLEM STATEMENT

Managing certificates the old fashioned way has certain drawbacks concerning the operation of the present system of certificate issuance and validation by institutions. Institutes usually give physical certificates to the students which are prone to be lost, damaged or even duplicated.

Now-a-days with readily accessible advanced digital tools; creating forged certificates has become a child's play. Employers and organizations have challenges in ensuring the certificates presented by the candidates are genuine as the current validation process is time consuming and usually involves calling the awarding body or using specialist 3rd party verification firms which can take weeks. It results into inefficiency of recruitment, organization among others.

The another important challenge is, there is no standardized system for certificate verification. Each organization has different verifications, but this creates more inconsistencies and inefficiencies in the validation. These challenges demand a secure, transparent and decentralized certificate validation system. This study proposes a blockchain-based cross-border e-health certificate validation system to address these challenges.

It uses blockchain technology to securely store information about the certificate, and QR codes for instantaneous permission and verification. Most importantly, it is impossible to fake the certificate as well as takes minimal time to verify.

III. OBJECTIVES OF THE STUDY

In this paper we propose a new blockchain based approach for efficient certification validation. In response to this need, we've designed a new system that has advantages over current methods of receiving/validating these credentials. The main goal is to create a decentralized certificate storage solution that guarantees the integrity and security of data. The system uses blockchain technology, making products unchangeable and undeletable once the certificate is stored within. Another goal is to shorten the time taken for certificate validation. The proposed system adds the use of QR code via which an employer or a verifier can scan and read information from certificate.

It also prevents certificate forgery by creating unique cryptographic hash values for every certificate saved in the blockchain. Because if there is any modification to the certificate, these hash values will be detected. Also, the proposed system aims to promote transparency and trust between educational institutions, students, and employers. Certificate structures are stored on a decentralized blockchain network, allowing all parties involved to access verified details of certificates without engaging intermediaries. Last but not least, the framework seeks to minimize admin burden and operational costs related to conventional certificate verification methods

IV. LITERATURE SURVEY

S.No	Author(s) & Year	Title of the Paper	Key Findings
1	Marco Valdi & Murat Yasin Kubilay (2021)	Generating E-Certificate and Validation using Blockchain	The study showed that blockchain can enhance certificate security and reduce dependency on centralized certificate authorities.
2	Nihu & Vani (2022)	Certificate Generation and Verification System Using Blockchain Technology Using QR Code	The system allows quick certificate verification by scanning QR codes and improves transparency in the verification process.
8	M. Perez & T. Wang (2022)	Leveraging Blockchain for Digital Credentialing	The study highlighted the benefits of blockchain in creating verifiable digital credentials.

V. PROPOSED SYSTEM

The proposed system is a Blockchain Based Certificate Validation System that helps in securely storing and validating the academic certificates. It enables academic institutions to grant digital certificates to their users, which get saved on the blockchain network post verification by an authorized administrator.

Students can submit their certificate details via a secure portal. After submission of the certificate, verification is performed by either institution's administrator or through an automated verification system. The verification is successful; now the information present in the certificate is changed into a digital format and stored over the blockchain network.

The certificate itself is linked to a unique cryptographic hash value that allows other people or entities to verify it. The certificate is also internally attached with a QR code which serves as an access key for validation. Upon scanning the QR code generated by the individual, an employer or verification authority would be redirected to a secure web portal, where the certificate details stored on the blockchain will be displayed.

In addition to this, the blockchain network guarantees that the details of a certificate will never be altered or modified as tampering is next to impossible on these networks. As the data is stored in a distributed manner across several nodes of the network, it has the potential to overturn cyber attacks and unauthorized changes.

Results: The proposed system improves the efficiency of certificate verification and significantly reduces the risk of fraudulent certificates. It also improves transparency by giving authorized users real time access to verified certificate information.

VI. SYSTEM ARCHITECTURE

There are mainly five components to this system. Students, colleges, administrator, blockchain nodes, verification authority. Students provide their certificate information to be stored on blockchain by uploading through certificate portal. Certificate portal is the user interface of this whole application that interacts with the blockchain network. College and administrator authorities verify the certificate. After the verification of the certificate, colleges store the certificates on the blockchain.

After storage college generates a hash value for the particular certificate data. Creates a new block with the help of that has value to store the information about certificate and add to the blockchain network. After a certificate gets verified, the system creates a hash value on it and creates a new block with the certificate's information.

The new block with certificate information will get pushed to blockchain network. All the blocks inside the blockchain network can't get altered, they are permanent.

Blockchain network consists of "nodes". Every node has a copy of distributed ledger. Nodes manage, validate and store data on the blockchain network. Since data is distributed across a large network of nodes, nobody can make any changes to the network which ensures security.
To Verify Certificates all employers or verifiers need to do is scan the QR code present on each certificate. QR code will lead you to the verification portal that fetches the certificate information from the blockchain. This makes storing certificates on blockchain an secure and fast verification process.

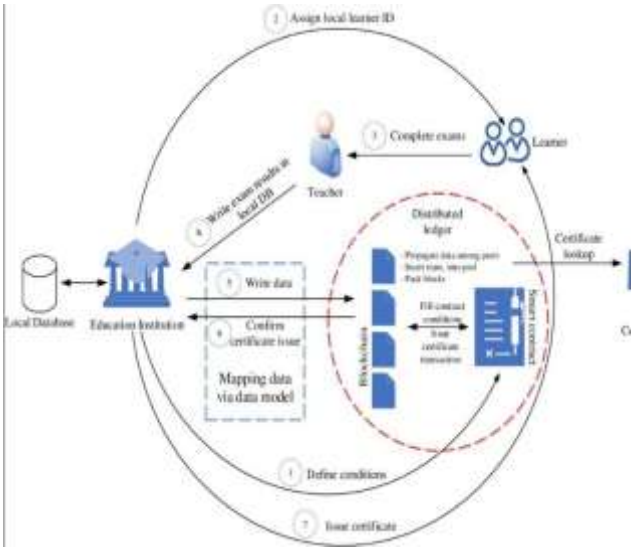

Figure 1: System Architecture of Blockchain-Based Certificate Validation System

VI. IMPLEMENTATION

The development of this blockchain-based certificate validation system will take place in various phases, which include system design, smart contract creation, blockchain network architecture, and user interface development.
Phase one includes performing a thorough analysis on what kind of system is needed based on requirements. First, what kind of certificates need to be validated? Then we must ask, what are the stakeholders that play major roles in the

validation process. The system involves various phases, from the design phase to the deployment phase.

During the design stage of the project, both the goals of the system and the needs of the end-users will be determined, and different possible options for the solution will be assessed. In the deployment stage of the project, the system will be deployed after addressing security considerations. The deployment will also be monitored for any potential vulnerabilities or interruptions. A secure login is used to authenticate students and the school to the system. The system utilizes access control to limit access based on a user's role. For example, an administrator's ability to verify certificates is limited, while a student's ability to provide the details of a certificate is restricted. APIs can aid in the connection between a website and the blockchain by allowing them to manage communications more easily. In addition to unit testing, integration testing, and system-level tests for demonstrating how well the system functions, there are other types of testing that help find security weaknesses. Implementations into the blockchain environment come after the results of these tests demonstrate a successful implementation of the project.

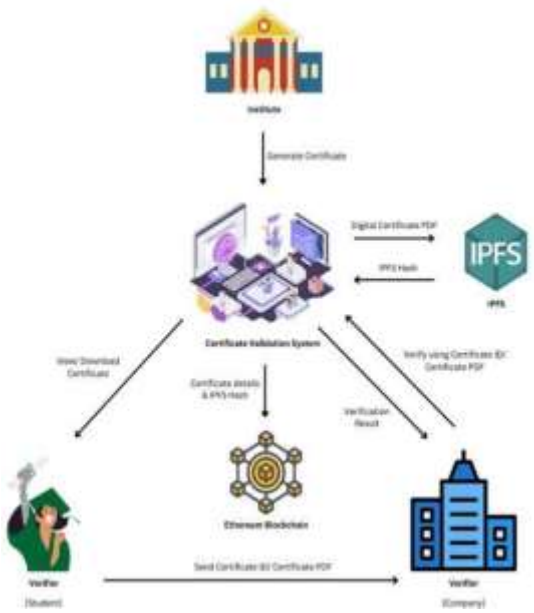

Figure 2 : Smart Contract Interaction in Certificate Validation System

VII. CONCLUSION AND RESULTS

Certificate management and verification services based on a blockchain framework to improve safety and efficient service for the end users. The services will improve safety in that tampering with and altering digital certificates will be impossible. The services will also implement verification procedures using QR Codes to reduce the manual burden associated with verification.

The services will create confidence and trust amongst those using certifying institutions, students and employers. The services will also reduce the chance of certificate forgery and reduce the time associated with the verification of certificates. The services will also maintain the decentralization and safety of the data associated with the services and the data of users of the services.

The services will answer the challenges associated with the processes of the verification of certificates. The solution will also provide a trustworthy service to users that will manage their digital credentials. The opportunities for further work will involve using Artificial Intelligence and Machine Learning to further improve the processes associated with certifying that digital certificates have not been altered. The work will also involve the processes associated with ensuring that digital certificates have not been altered.

REFERENCES

1. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
2. Tariq, H. B. Haq and S. T. Ali, “Cerberus: A Blockchain-Based Accreditation and Degree Verification System,” IEEE Transactions on Computational Social Systems, 2019.
3. Rahman, S. I. Mouno, A. M. Raatul and A. K. Al Azad, “Verifi-Chain: A Credentials Verifier Using Blockchain and IPFS,” 2023.
4. E. Andrade and F. C. Amate, “A Decentralized Academic Certificate Issuance System Using Smart Contracts on the TRON Network,” 2026.
5. Khati, A. K. Shrestha and J. Vassileva, “Student Certificate Sharing System Using Blockchain and NFTs,” 2023.

6. S. H. Said, "A Blockchain-Based Conceptual Model to Address Academic Certificate Verification Challenges," Engineering, Technology & Applied Science Research, 2023.
7. S. K. Patel, "Secure Digital Academic Certificate Verification System Using Blockchain Technology," International Journal of Information and Communication Security, 2024.
8. O. S. Oluwaseyi, "Utilizing Blockchain Technology for University Certificate Verification Systems," International Journal of Artificial Intelligence & Applications, 2024.
9. VIII. Ifeyemi, "A Blockchain-Based Digital Educational Certificate Verification System,"
10. Journal of Engineering Technology and Innovation, 2024. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," IEEE Access, 2023.
11. S. Gangwar et al., "Blockchain-Based Authentication and Verification System for Academic Certificates Using QR Code," International Journal of Computer Applications, 2024.
12. Sree et al., "Decentralized Certificate Issuing and Verification System Based on Ethereum Blockchain," ScienceDirect, 2025.
13. C. Rashmi et al., "Decentralized Academic Certificate Issuance and Verification Using Blockchain Technology," IJSREM, 2025.
14. D. et al., "Secure Academic Certificate Authentication Using Ethereum Smart Contracts and IPFS," SSRN, 2025.
15. Bhise et al., "Blockchain Based Certificate Validation System," International Journal for Multidisciplinary Research (IJFMR), 2025.
16. Sari and T. Gelar, "Prototype of Blockchain-Based Diploma Transcript Authentication Method," 2025.
17. Singh et al., "Blockchain-Based Certificate Validation Framework," IEEE Conference on Blockchain Technologies, 2018.
18. Iyer et al., "A Secure Certificate Validation System Using Blockchain
19. Technology," IEEE International Conference on Distributed Systems, 2019.
20. Kim et al., "Blockchain-Based Certificate Validation for IoT Devices," IEEE Internet of Things Journal, 2020.
21. Gupta et al., "Decentralized Certificate Validation System Using Blockchain,"
22. International Journal of Computer Science and Network Security, 2021.