

Generation and Validation of Certificates Using Blockchain

Mrs.P.Brundha *, C.Aldrin Graceson **, V.Benjamin Zechariah ***

*(Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli
Email: brundha.p@francisxavier.ac.in)

** (Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli
Email: aldringracesonc.ug22.cs@francisxavier.ac.in)

*** (Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli
Email: benjaminzechariahv.ug22.cs@francisxavier.ac.in)

Abstract:

Conventional certificate management systems are vulnerable to loss, fraud, and verification inefficiencies. This project uses blockchain technology to develop a decentralised, safe, and unchangeable system for digital certificate issuance, storage, and verification. Each certificate is saved on the blockchain using cryptographic hashing, which guarantees validity and guards against manipulation. Certificates are transparently recorded by issuers and are securely accessible and shared by recipients. Instantaneous verification eliminates the need for middlemen. The platform offers a smooth and fraud-proof solution with Ethereum-based authentication, like MetaMask, improving efficiency and confidence in digital credential management.

Keywords — Blockchain, Digital Certificate, Ethereum, Smart Contract, SHA-256 Hashing, Decentralized Identity, Web3, Certificate Authentication, Tamper-Proof Records, Immutable Ledger, MetaMask, Cybersecurity, Solidity, Digital Credentials, Trustless Verification

I. INTRODUCTION

The validity, security, and integrity of digital certificates have grown in significance in the contemporary digital era across a variety of industries, including government, employment, education, and training facilities. Due to their heavy reliance on centralised authorities, traditional certificate management systems are susceptible to data loss, falsification, tampering, and restricted accessibility. These traditional methods frequently lack transparency and call for laborious, ineffective, and prone to human error manual verification procedures.

Blockchain technology offers a revolutionary solution to these problems by

providing a decentralised, transparent, and unchangeable digital certification infrastructure. In order to safely issue, store, and authenticate digital certificates—and guarantee that they cannot be changed or falsified once they are issued—this project makes use of Ethereum-based smart contracts. Data integrity and verifiability are ensured by incorporating cryptographic hashing, which transforms each certificate's contents into a distinct SHA256 hash and stores it on the blockchain indefinitely.

Additionally, both issuers and recipients can have safe and easy access control when Ethereum wallet addresses are used for authentication. By doing away with the need for middlemen, this decentralised system not only

improves trust and dependability but also makes verification easier for third parties. The end result is a user-controlled, tamper-proof system that gives people and organisations digital credentials that are universally accessible, long-lasting, and verifiable.

II. OBJECTIVES

Addressing the difficulties that conventional certificate issuance and verification systems encounter is at the heart of this project's goals. These systems frequently have problems such as ineffective validation procedures, centralised control, lack of transparency, and forgeries. A secure, decentralised, and impenetrable solution is urgently needed due to the growing dependence on digital documents in the corporate and educational sectors. To satisfy these requirements, this project makes use of the benefits of blockchain technology, including immutability, decentralisation, and transparency. The primary aims of this innovation are delineated by the subsequent objectives

- To create and put into use a blockchain-based certificate management system that guarantees non-repudiation and validity.
- Keeping cryptographic hashes of certificates on the Ethereum blockchain will stop certificate forgeries.
- To validate certificates in an independent and decentralised manner using smart contracts.
- To enable safe Ethereum wallet integration (e.g., MetaMask) so that users (issuers and recipients) can communicate with the system.
- To reduce the dependence on centralised authorities for certificate validation and verification.
- To offer an easily adoptable platform for certificate verification that is transparent, scalable and open to the public for use by corporations, recruiters, and educational institutions.
- To protect data privacy, sensitive information should be off-chain yet

verifiable, and only hash values should be stored on-chain

III. MODULES AND ALGORITHM

When it comes to software development, a module is a discrete, independent functional unit that supports the system's overarching goal. Modules in a blockchain-based certificate management platform are made to separate the system into logical sections, each of which is responsible for particular tasks such as data validation, blockchain interaction, user authentication, and certificate issuance. The application's maintainability, scalability, and clarity are improved by this modular structure, which makes it possible to build and debug individual components independently. The main modules used in this project are listed below:

Modules

A. User Authentication Module:

This module is in charge of using MetaMask to validate users' Ethereum wallet usage. It guarantees that certificates can only be generated by verified issuers and that recipients can safely access them without the need for traditional usernames or passwords.

1. Certificate Issuance Module:

It is responsible to create digital certificates. Before being stored on the blockchain, data entered by issuers is analysed and transformed into a SHA-256 hash to guarantee its integrity.

2. Smart Contract Module:

This module, which is implemented in Solidity, offers features for storing and retrieving certificate hashes on the blockchain. It ensures clear access to verification data and immutability.

3. Certificate Validation Module:

By comparing freshly calculated hashes with those kept on the blockchain, this module enables end

users and outside parties to confirm the legitimacy of certificates.

4. Backend Database Module:

This off-chain module uses SQLite to store system logs, certificate metadata, and user profiles. By facilitating effective data management without requiring expensive gas prices, it enhances the blockchain.

5. Frontend Interface Module:

This module serves as the primary user interface and was constructed with React.js. Its user-friendly and responsive design enables users to issue and view certificates, connect their wallets, and carry out validation.

B. Algorithm

The project's algorithm starts with the issuer linking their Ethereum wallet to the site (via MetaMask). After that, the issuer inputs certificate data, which is hashed to guarantee its integrity using the SHA-256 hashing technique. The Ethereum blockchain's smart contract receives this hash and stores it immutably, linking it to a distinct certificate ID. Metadata, such as user ID and event information, is stored in the backend database for convenient access. To verify authenticity, the hash of the certificate data is compared with the hash stored on the blockchain when a certificate is sought for validation. Transparency, security, and confidence in the certificate validation procedure are guaranteed by this decentralised, impenetrable system.

IV. METHODOLOGIES

A. Blockchain Technology:

The project makes use of blockchain technology, particularly Ethereum, to guarantee decentralisation, transparency, and immutability. To prevent data

manipulation after issue, smart contracts are used to store digital certificate hashes on the blockchain.

B. Smart Contract Deployment:

The Ethereum blockchain uses smart contracts to manage the hashed certificate data's storage and retrieval. This offers a decentralised method of certificate verification and does away with the requirement for a central authority.

C. SHA-256 Hashing:

Prior to being put in the smart contract, the certificate data is hashed using the SHA-256 technique. Because of this cryptographic hashing, any manipulation will be immediately identifiable because the hash value will change even if the original data is altered.

D. MetaMask Integration:

To manage user authentication using their Ethereum wallets, the project incorporates MetaMask. This makes it possible for issuers and recipients to safely communicate with the system and confirm certificate details straight from the blockchain.

E. API Development:

The blockchain is accessed, and certificate info is retrieved using a RESTful API. This API makes it possible for the client and backend to communicate seamlessly, which makes it easier to issue and validate certificates in an approachable way.

F. Decentralised Storage:

Instead of being stored in a centralised database, the data is decentralised on the blockchain, minimising the possibility of data manipulation and guaranteeing that there is no single point of failure.

G. Frontend Development with React.js:

React.js is used to provide a responsive UI that makes it simple for users to browse issued certificates, interact with the platform, and check their legitimacy by submitting a blockchain query.

H. Database Integration:

The user interface may be quickly and effectively retrieved by using a local SQL database that has metadata about the certificates, including user and event details.

V. EXISTING SYSTEM

To issue and validate certificates, the present certificate management system mostly depends on centralised authority, including government agencies, corporate enterprises, and educational institutions. These certificates are frequently kept in internal record systems or local databases and are typically offered in hard copy or as digital PDFs. Direct communication with the issuing authority is necessary for the verification of these documents, although doing so can be laborious, ineffective, and subject to manipulation. Furthermore, because the issuing agency alone controls and maintains the underlying data, there is little accountability or transparency.

1. Centralised Control and Storage:

In order to issue and maintain certificates, the present certificate management system mostly relies on centralised entities like businesses, government agencies, and universities. These certificates are typically kept on issuer-controlled local servers or file systems, which introduces a single point of failure and raises questions about data security and integrity.

2. Manual Validation:

In the conventional system, verifying certificates is frequently a laborious and manual process. To verify the document's legitimacy, it usually entails getting in touch with the issuing authorities by phone, letter,

or email. This causes delays and mistakes and slows down procedures like employment, admissions, and document authentication.

3. Risk of Forgery and Tampering:

Certificates can be easily falsified, altered, or copied without permission because they are frequently sent as hard copy papers or unprotected digital files (like PDFs). The trust of legitimate credentials is weakened by the lack of protection against fraud.

4. Limited Accessibility and User Control:

Certificate holders have little control over their own credentials under the current configuration. There is no centralised infrastructure for handling papers produced by various organisations, and they depend on issuers to retrieve or resend certificates as needed. Portability and convenience of use are hampered by this lack of accessibility.

5. Lack of Interoperability:

There is no uniform system for confirming papers across institutions or nations since every entity issues and maintains certificates using its own internal procedure. Ineffectiveness and mistrust in international academic and professional mobility are caused by this lack of interoperability.

PROPOSED SYSTEM

Using blockchain technology, the proposed system seeks to completely transform the issuance, verification, and storage of digital certificates. This solution guarantees a safe, unchangeable, and transparent approach to certificate management, in contrast to conventional centralised systems that are vulnerable to fraud, manipulation, and data loss. Since every certificate is hashed and kept on a blockchain, anyone can confirm its legitimacy without having to access the database kept by the issuing authority. The system is decentralised and safely available to issuers and recipients thanks to

the integration of MetaMask for Ethereum-based interactions.

A. Certificate Issuance On-chain:

A safe, decentralised system in which the details (hashed data) are kept on a blockchain and certificates are issued by authorised parties. This removes the possibility of fraud or manipulation and guarantees the legitimacy of certificates. The creation and administration of certificates will be automated through the use of smart contracts.

B. Decentralised Certificate Validation:

By comparing a certificate's hash with the blockchain data, this technique enables beneficiaries, employers, or other third parties to confirm a certificate's legitimacy. Without depending on centralised agencies or manual procedures, the immutable and transparent nature of blockchain guarantees that certifications are legitimate and verifiable.

C. Smart Contract-Driven Authentication:

Certificate issuance and retrieval will be controlled by smart contracts. To make sure that only authorised people may produce legitimate certificates, issuers—such as colleges or organisations—will use MetaMask to confirm their identities. Once specific requirements are fulfilled, these contracts will immediately start the certificate creation process.

D. User-Friendly Web Interface for Beneficiaries:

Beneficiaries will be able to view their issued certificates on a web-based platform. They will be able to safely log in and view or share their certificates thanks to MetaMask integration. Accessing and interacting with blockchain data will be simple because of the user-friendly interface.

E. Scalable and Integrative Platform for Enterprises:

This system's scalable design enables corporate entities, educational institutions, and other certifying authorities to issue certificates in large quantities. Additionally, it offers APIs for platform integration, which facilitates the adoption and use of the blockchain certificate system by companies and academic institutions.

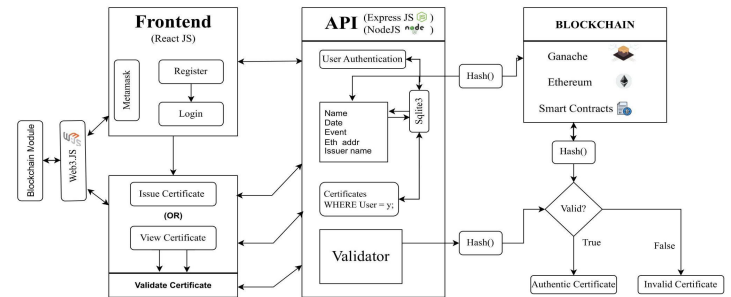


Figure 1: Architecture Diagram

VI. OUTPUT

The output of the suggested system covers a number of important areas, showing how the blockchain-based certificate management platform improves certificate security, validity, and transparency.

A. Issuance of Blockchain-Backed Certificates:

The issuing of certificates that are safely kept on the blockchain is the system's main output. To prevent tampering, a certificate's hash is stored on the blockchain after it is generated. Unique metadata, including the certificate ID, recipient, issuer, and event, are linked to each certificate and are encrypted to guard against unwanted access.

technology's decentralised and unchangeable features, the system makes sure that certificates are unchangeable, eliminating fraud and guaranteeing the accuracy of credential verification.

The use of smart contracts automates certificate issuance, making the process faster and more efficient for both issuers and beneficiaries. This reduces administrative overhead and ensures that certificates are generated only under valid conditions. Furthermore, the transparency offered by blockchain allows anyone to easily verify a certificate's authenticity without the need for a third-party intermediary, reducing both cost and time.

Unlike previous fake face identification algorithms, which frequently rely on static datasets and lack real-time adaptability, our method exhibits better generalisation across a wide range of photos and situations. It successfully bridges the gap between technical robustness and user-centric design, ensuring that even while synthetic media continues to change, the system remains an effective tool for detecting and preventing misuse.

Overall, the created Fake Face Detection system is a big step in developing dependable and scalable solutions for digital media authenticity. Its modular and extensible architecture offers the framework for ongoing study and innovation, making it a great contender for wider deployment in applications where security, trust, and the integrity of digital identity are critical.

VII. ACKNOWLEDGMENT

We would like to express our sincere gratitude to our project guide, Ms. P. Brundha, Assistant Professor, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, for her invaluable support, guidance, and encouragement throughout the duration of this project. Her insights and continuous motivation played a crucial role in shaping our ideas and bringing the project to fruition. We also extend our heartfelt thanks to the faculty and management of the Department of Computer Science and Engineering for providing the resources and environment necessary for the successful

completion of our work. We, Aldrin Graceson and Benjamin Zechariah, are deeply thankful for the opportunity to work under her guidance and for the collaborative learning experience this project has provided.

REFERENCES

- [1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.
- [2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008
- [3] A. Al-Bassam, "SCPKI: A Smart Contract-Based PKI and Identity System," in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Abu Dhabi, UAE, 2017, pp. 35–40, doi: 10.1145/3055518.3055522.
- [4] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
- [5] M. Sharples and J. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation, and Reward," in Proceedings of the 11th European Conference on Technology Enhanced Learning (EC-TEL), Lyon, France, 2016, pp. 490–496, doi: 10.1007/978-3-319-45153-4_48.
- [6] A. Grech and A. F. Camilleri, "Blockchain in Education," Joint Research Centre (JRC) Technical Reports, European Commission, 2017.
- [7] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, 2014.
- [8] Y. Zhang and J. Wen, "The IoT Electric Business Model: Using Blockchain Technology for the Internet of Things," in Peer-to-Peer Networking and Applications, vol. 10, no. 4, pp. 983–994, July 2017, doi: 10.1007/s12083-016-0456-1.
- [9] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," 1996.

- [10] S. Chen, R. Shi, H. Ren, J. Yan, and Y. Shi, "A Blockchain-Based Educational Record Repository," in 2018 IEEE 18th International Conference on Advanced Learning Technologies (ICALT), Mumbai, India, 2018, pp. 385–387, doi: 10.1109/ICALT.2018.00096.