e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 10, October 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 10, October 2024| DOI: 10.15680/IJMRSET.2024.0710048

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Developing a Blockchain Based Certificate Verification System

Muthuvairavan Pillai N[1] Shaileshh C[2], Sanjay Aditya S [3], Viswa[4]

Associate Professor, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India[1]

Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India[2]

Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India[3]

Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India[4]

ABSTRACT: The increasing prevalence of forged academic and professional certificates has led to a pressing need for secure, transparent, and tamper-proof verification mechanisms. Traditional certificate verification processes are often time-consuming, costly, and prone to inefficiencies. This paper presents a blockchain-based certificate verification system that leverages the decentralized, immutable, and transparent properties of blockchain technology to address these challenges. In this system, academic institutions and certifying authorities issue digital certificates, which are stored on a public or private blockchain. Each certificate is cryptographically signed and permanently recorded on the blockchain, ensuring its authenticity and preventing any unauthorized modifications. Employers, educational institutions, or other verifying bodies can easily access and verify the validity of the certificate in real-time, without the need for intermediaries. This paper explores the design, implementation, and potential applications of blockchain in the certificate verification process, highlighting its benefits and addressing possible challenges. In conclusion, the blockchain-based certificate verification system presents a transformative approach to credential management, paving the way for secure, transparent, and efficient verification processes that can benefit a wide range of industries.

I. INTRODUCTION

A blockchain-based certificate verification system leverages the decentralized, secure, and immutable nature of blockchain technology to revolutionize how academic and professional certificates are issued, verified, and managed. Traditional systems for managing certifications are prone to inefficiencies, security risks, and susceptibility to fraud, requiring trusted intermediaries to verify credentials. However, with a blockchain-based solution, certificates are securely stored on a distributed ledger, ensuring transparency, immutability, and accessibility. This system eliminates the need for intermediaries and provides verifiable and tamper-proof certificates that can be authenticated by anyone in real-time. It also ensures the privacy of individuals, as only authorized parties can access personal details associated with the credentials. Blockchain technology ensures that once a certificate is issued, it cannot be altered or deleted, making it highly resistant to fraud. Additionally, the decentralized nature of blockchain means there is no single point of failure, ensuring availability and security of the data. Such a system streamlines the verification process for employers, academic institutions, and individuals, reducing administrative burdens while enhancing trust and security.

II. LITERATURE SURVEY

[1] Omar S. Saleh, Osman Ghazali, Muhammad Ehsan Rana (2020).
Blockchain-Based Framework for Educational Certificates Verification.
This paper proposes a blockchain-based framework using Hyperledger Fabric for secure verification of educational certificates. It addresses issues in traditional verification processes like fraud, forgery, and inefficiency. The framework emphasizes five key security themes: authentication, authorization, confidentiality, privacy, and ownership. Hyperledger Fabric, a permissioned blockchain, ensures role-based access, privacy, and transparency, enabling a tamper-proof system for issuing, managing, and verifying educational credentials.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[2] Elva Leka and Besnik Selimi (2021):

Development and Evaluation of Blockchain-Based Secure Application for Verification and Validation of Academic Certificates.

The paper introduces a blockchain solution using Ethereum for secure storage and verification of academic certificates. It utilizes smart contracts to automate the verification process, eliminating intermediaries and improving efficiency. The system comprises three components: a verification application for certificate validation, a university interface for issuing certificates, and an accreditor interface to ensure only validated institutions can issue certificates. The system prioritizes privacy, security (with AES encryption), and supports bulk submissions.

[3] Ravi Singh Lamkoti, Devdoot Maji, Hitesh Shetty, Prof. Bharati Gondhalekar (2021):

Certificate Verification Using Blockchain and Generation of Transcript.

This paper presents a blockchain-based system for generating and verifying digital academic certificates to prevent tampering and forgery. Using the Ethereum blockchain and smart contracts, certificates are issued with unique hash keys, stored securely using the InterPlanetary File System (IPFS). This approach ensures immutability and transparency, allowing easy detection of any tampering attempts.

[4]Binh Minh Nguyen, Thanh-Chung Dao, Ba-Lam Do (2020):

Towards a Blockchain-Based Certificate Authentication System in Vietnam.

The paper addresses counterfeit educational certificates in Vietnam with the proposed VECefblock system. Using blockchain's capabilities such as anti-forgery, transaction verification, and smart contracts, the system enhances data transparency and integrity. It includes an analysis of blockchain trends, system architecture, data mapping, and implementation on Hyperledger Fabric. Tested on Amazon EC2, the paper demonstrates blockchain's feasibility in addressing challenges in certificate authentication.

[5] Dinesh Kumar K, Senthil P, Manoj Kumar D.S (2020):

Educational Certificate Verification System Using Blockchain

This paper proposes a blockchain-based system to improve academic certificate verification processes, overcoming issues like delays, errors, and fraud. Using Ethereum blockchain and cryptographic hashing, certificates are stored in a tamper-proof, immutable format. Smart contracts automate the verification process, ensuring transparency, security, and faster certificate verification for both employers and educational institutions.

III. EXISTING SYSTEM

Current systems for issuing and verifying certificates rely on traditional paper-based or centralized digital methods, where institutions manually issue certificates and verifiers must contact them to confirm authenticity. 1. Paper-Based Certificate System In this system, institutions such as universities, training providers, or professional bodies issue physical certificates. Once printed, they are delivered to individuals (graduates, employees, etc.), who then store them as proof of their qualifications. When employers or other institutions require verification, they must contact the certificate-issuing body directly, often through emails, letters, or phone calls. 2. Centralized Digital Certificate Systems Many institutions have adopted digital methods for issuing certificates, using centralized databases where these credentials are stored. These digital systems allow institutions to generate electronic versions of certificates that can be shared or accessed by certificate holders. However, verifiers often need to access this central database or request confirmation from the issuing institution to check the certificate's authenticity. Drawbacks of the Existing System 1. Fraud and Forgery: - Paper certificates are vulnerable to counterfeiting, while centralized digital systems are prone to hacking and data manipulation. 2. Time-Consuming Verification: - Verifying certificates through institutions involves manual processes that can take days or weeks, causing delays in hiring, admissions, or credential validation. 6 3. High Administrative Costs: - Manual processes for issuing and verifying certificates are labor-intensive and prone to human errors, increasing operational costs for institutions. 4. Data Vulnerabilities: - Paper certificates are at risk of damage or loss, while centralized digital systems are susceptible to data breaches, hacking, or server failures, creating a single point of failure. 5. Limited Accessibility and Interoperability: - Paper certificates are hard to verify across borders, and digital systems are often incompatible across institutions, making verification difficult for international or multi-institutional cases. 6. Inconsistent Trust and Reliability: - Institutions' reputations vary, and manual verification may not guarantee reliability, especially when dealing with unfamiliar or international institutions.

© 2024 IJMRSET | Volume 7, Issue 10, October 2024| DOI: 10.15680/IJMRSET.2024.0710048

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. PROPOSED SYSTEM

The proposed blockchain-based certificate verification system leverages blockchain technology to address the challenges of traditional certificate issuance and verification systems. By introducing a decentralized, secure, and transparent platform, the system aims to revolutionize the way certificates are managed, ensuring tamper proof records and real-time verification. Advantages of the Proposed System 1. Fraud Prevention: The use of Blockchain immutability ensures that certificates cannot be forged or altered after issuance. 2. Instant and Global Verification: Employers and institutions can verify certificates in real-time without relying on the issuing institution, speeding up processes and enabling cross-border verification. 3. Cost Efficiency: Automation reduces the need for administrative staff to manually issue and verify certificates, cutting down operational costs. 4. Enhanced Trust: Blockchain s transparency and auditability create a system that fosters trust between certificate issuers, holders, and verifiers.

V. METHODOLOGY OF APPROACH

System Specifications:

- **Software:** Anaconda, Python 3.7+, Notepad/MS Word, 64-bit OS, Windows 7+, Visual Studio Code.
- **Hardware:** Core i5 processor or higher, 8GB RAM

Architecture Diagram

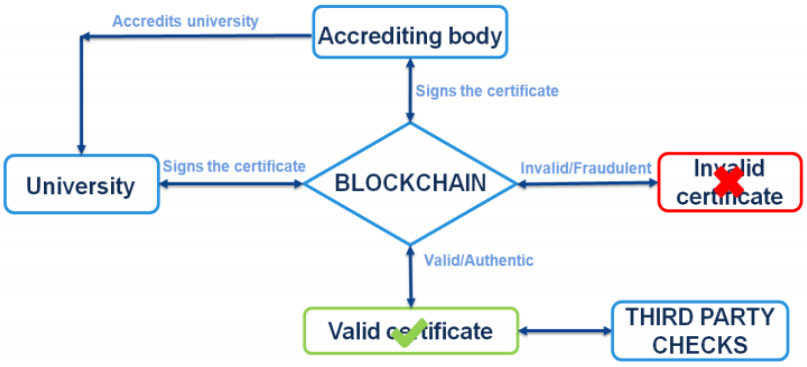

Figure 1. Architecture of issuing certificates

User Authentication:

- Sign-Up/Log-In Process: Users register by providing personal details such as name, email, and password. Returning users log in with their credentials.
- Backend Verification: User credentials are sent to the backend for verification against a stored database. If valid, the user is authenticated.
- Authorization Token: Upon successful authentication, the backend generates a unique authorization token for secure communication in subsequent API requests.
- Role Assignment: Users are assigned roles (e.g., institution, employer, verifier) with different access rights based on their profile.

Certificate Issuance:

- Issuance Mechanism: After logging in, authorized users can issue certificates through the frontend interface, including necessary details like certificate type, recipient, and issuer.
- Hashing Process: The backend generates a cryptographic hash of the certificate to ensure integrity, with the hash serving as a unique identifier.
- Off-Chain Storage: To optimize costs, actual certificates are stored off-chain using secure cloud storage or IPFS.
- Blockchain Recording: The hash and metadata (e.g., recipient, timestamp) are sent to the blockchain, where a smart contract stores this information for transparency and immutability

© 2024 IJMRSET | Volume 7, Issue 10, October 2024| DOI: 10.15680/IJMRSET.2024.0710048

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Certificate Verification:

- User Selection: When verifying a certificate, users specify the certificate ID or details.
- Verification Process: The system queries the blockchain for the corresponding hash and metadata, validating its authenticity.
- Frontend Display: Verified data is displayed to users, allowing them to view certificate details and status.

Role-Based Access Control:

- Smart Contract Role Management: Smart contracts enforce role-based access control, determining who can issue or verify certificates.
- Permission Levels: Permissions are defined based on user roles, ensuring that only authorized entities can perform specific actions (e.g., issuing, verifying).
- Enforcement: Any actions taken are verified by smart contracts to ensure compliance with permission settings, blocking unauthorized attempts.

Certificate Retrieval:

- Certificate Listing: Users can view all certificates they are authorized to access. The backend validates the user's authorization token before querying the blockchain for certificate hashes and metadata.
- Frontend Display: Retrieved data is presented in a user-friendly format, allowing users to manage and download their certificates.

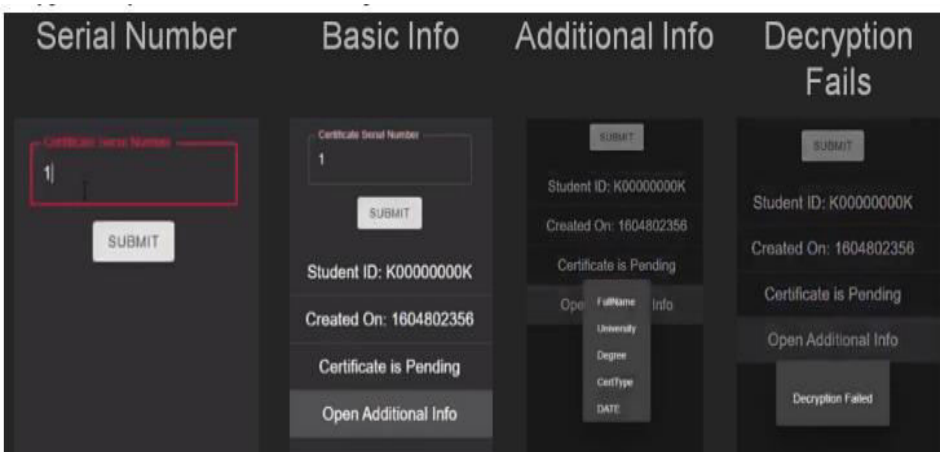

FIG 2: VERIFICATION PROCESS

Dispute Resolution:

a. Certificate History: In cases of disputes regarding ownership or authenticity, the blockchain serves as an immutable record of all certificate-related transactions.
b. Verification of Ownership: Smart contracts manage ownership and access permissions, aiding in the resolution of disputes over certificate validity.
c. Transparent Audit Trail: All actions involving a certificate (issuing, verification, etc.) are logged on the blockchain, providing a clear audit trail for verification.

Third-Party Integration:

a. API Integration: The system includes APIs for external services (e.g., educational databases, employers) to verify certificates, contingent on security and role-based access.
b. Smart Contract-Based Authorization: Smart contracts handle API permissions, ensuring third-party access only occurs with user consent and proper authorization.
c. KYC as a Service: Third-party KYC services are integrated to verify user identities while maintaining privacy, facilitating secure certificate verification.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. RESULT AND DISCUSSION

The blockchain-based certificate verification system offers a robust and secure platform for issuing and validating academic and professional certificates. By leveraging blockchain technology, the system ensures the integrity and immutability of certificates, protecting against unauthorized alterations. The user-friendly interface enhances user experience and facilitates efficient communication among stakeholders. With a well-designed backend API, the system allows real-time updates and collaboration, making it scalable and adaptable across various sectors. Prioritizing data security, transparency, and reliability, this solution significantly improves the verification process, benefiting educational institutions, employers, and individuals.

VII. FUTURE ENHANCEMENTS

1. **Enhanced Security and Privacy**
- Zero-Knowledge Proofs (ZKP): Implementing ZKP can validate certificate authenticity without exposing sensitive data, enhancing user privacy.
- Multi-Party Computation (MPC): MPC would allow secure joint computations of sensitive data, improving confidentiality in certificate management.
- Quantum-Resistant Cryptography: Adopting quantum-resistant algorithms will safeguard against future quantum computing threats.

2. **Interoperability and Cross-Chain Functionality**
- Cross-Chain Bridges: These will facilitate communication between different blockchain networks, allowing seamless certificate verification across platforms.
- Universal Data Standards: Standardized formats will enhance compatibility with other systems, improving data exchange.

3. **Smart Contract Automation and Self-Executing Protocols**
- Automated Certificate Lifecycles: Smart contracts could automate expiration and renewal processes for certificates, enhancing compliance and efficiency.
- Event-Driven Automation: Implementing triggers based on conditions (e.g., expiry notifications) would streamline operations and reduce manual tasks.

VIII. CONCLUSION

Implementing a blockchain-based certificate verification system offers numerous advantages, including enhanced security, transparency, and efficiency in credential management. The decentralized and immutable nature of blockchain ensures the integrity of certificates, protecting them against fraud and unauthorized access. By digitizing the verification process and automating tasks through smart contracts, organizations can streamline operations and reduce administrative burdens. The system also facilitates compliance with regulatory requirements, providing a secure and auditable solution for credential management. Overall, this innovative approach has the potential to revolutionize how academic and professional certificates are issued, verified, and managed, fostering trust and efficiency across diverse industries.

REFERENCES

[1]Omar S. Saleh, Osman Ghazali, Muhammad Ehsan Rana - "Blockchain Based Framework for Educational Certificates Verification" published in *Journal of Critical Reviews, Vol 7, Issue 3, 2020* (Blockchain_Based_Frameworks).

[2]Elva Leka, Besnik Selimi - "Development and Evaluation of Blockchain based Secure Application for Verification and Validation of Academic Certificates" published in *Annals of Emerging Technologies in Computing (AETiC), Vol. 5, No. 2, 2021*(p3).

[3]Ravi Singh Lamkoti, Devdoot Maji, Prof. Bharati Gondhalekar, Hitesh Shetty - "Certificate Verification using Blockchain and Generation of Transcript" published in *International Journal of Engineering Research & Technology (IJERT), Vol. 10 Issue 03, March-2021*(IJERT_Certificate_Verification).

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[4]Nachiappan Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman - "BlockChain Technology: Beyond Bitcoin" published in *Applied Innovation Review, No. 2, June 2016*.

[5]Tarek Kanan, Ahamd Turki Obaidat, Majduleen Al-Lahham - "SmartCert BlockChain Imperative for Educational Certificates" published in *Electrical Engineering and Information Technology (JEEIT), 2019 IEEE Jordan International Joint Conference, pp. 629-633, 2019*.

[6]Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Guiseppe Gottardi - "Certificate Validation through Public Ledgers and Blockchains" published in *Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy, 2017*.

[7]Jiin-Chiou, Narn-Yih Lee, Chien Chi, Yi-Hua Chen - "Blockchain and Smart Contract for Digital Certificate" published in *Proceedings of IEEE International Conference on Applied System Innovation, 2017*.

[8]Xiuping Lin - "Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the Ethereum Blockchain" published by *Department of Information Engineering, National Taiwan University, Taiwan, R.O.C., 2017*

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com