Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 5, May 2024

E-Certificate Verification Using Blockchain

Nupur Vikhankar, Ankita Andhare, Ishwari Barne,
Prof. Anand Dhawale, Sadaf Kauchali
Dept. of Computer Engineering,
Modern Education Society's
Wadia College of Engineering, Pune

Abstract:
This research paper presents a comprehensive study on the implementation of blockchain technology for certificate verification, aiming to address the growing concerns regarding the authenticity and reliability of academic credentials. The proposed system utilizes Ethereum blockchain, MetaMask wallet, and Ganache for seamless deployment and interaction. Key functionalities include institution registration, certificate issuance, verification, and revocation, all facilitated through a user-friendly interface featuring two tabs: "Verification" and "Issue Certificate". Institutions register by providing details such as institution name, website, and courses offered, deploying smart contracts using Ether from MetaMask. Subsequently, certificates are generated for students, each associated with a unique hash key, ensuring tamper-proof verification. The verification tab enables users to validate certificates by entering the unique key. Additionally, the system offers a revocation option for invalid certificates. This paper contributes to the blockchain literature by offering a practical and secure solution for certificate verification, addressing the pressing need for trust and transparency in academic credentials. The verification of academic certificates is a critical aspect of ensuring the authenticity and credibility of individuals' qualifications. Traditional methods of certificate verification often face challenges such as fraud, manipulation, and inefficiency. In our research paper, we introduce an innovative method for certificate verification utilizing blockchain technology. Our system offers a reliable and transparent way for institutions to issue certificates and for recipients to confirm their validity. By harnessing smart contracts and decentralized agreement mechanisms, we showcase the transformative potential of blockchain in redefining the management and validation of academic qualifications.

Keywords: **Blockchain, Certificate Verification, Ethereum, MetaMask, Smart Contracts, Academic Credentials**

1.INTRODUCTION

In today's digital era, the verification of academic certificates holds paramount importance in various spheres including education, employment, and professional accreditation. However, the traditional methods of certificate verification are often plagued with issues such as fraud, manipulation, and lack of transparency. To tackle these obstacles, this study introduces an innovative method utilizing blockchain technology for certificate verification. Initially created to support cryptocurrencies, blockchain has garnered widespread adoption in diverse sectors thanks to its decentralized, transparent, and immutable nature. By leveraging these attributes, blockchain presents an effective means to bolster the security and dependability of certificate verification procedures.The proposed certificate verification system utilizes Ethereum blockchain, MetaMask wallet, and Ganache for seamless deployment and interaction. The system features a user-friendly interface with two tabs: "Verification" and "Issue Certificate". Institutions can register by providing details such as institution name, website, and courses offered. Upon registration, smart contracts are deployed using Ether from the MetaMask wallet, ensuring secure and transparent transactions.

Subsequently, institutions can generate certificates for students, each associated with a unique hash key, thus ensuring tamper-proof verification. The verification tab allows users to validate certificates by entering the unique key, providing a robust mechanism to verify the authenticity of academic credentials.. Moreover, the system offers an option for revoking certificates in case of invalidity, thereby further enhancing trust and reliability. This paper aims to contribute to the existing literature by presenting a comprehensive framework for certificate verification using blockchain technology. Through empirical analysis and real-world implementation, we demonstrate the efficacy and potential of blockchain in revolutionizing the certificate verification process, thereby addressing the pressing need for trust and transparency in academic credentials.

2.MOTIVATION

The verification of academic certificates plays a pivotal role in ensuring the credibility and authenticity of individuals' qualifications. However, traditional methods of certificate verification often face challenges such as fraud, manipulation, and inefficiency. These challenges pose significant risks to various stakeholders, including educational institutions, employers, and individuals seeking to validate their credentials. The motivation behind this research stems from the pressing need to address these challenges and develop innovative solutions that enhance the trust and transparency of certificate verification processes. Blockchain technology presents an encouraging pathway to address these challenges by furnishing a decentralized and immutable ledger to securely record transactions.

By leveraging blockchain technology, we aim to revolutionize the certificate verification process, making it more secure, transparent, and efficient. The proposed system not only mitigates the risk of fraud and manipulation but also simplifies the verification process for all stakeholders involved .Moreover,

the decentralized structure of blockchain guarantees that no individual entity holds authority over the verification process, diminishing dependence on centralized bodies and cultivating trust among participants. This decentralization also promotes increased transparency, as every transaction is logged on a publicly accessible ledger, available to all relevant parties..
Overall, the motivation behind this research is to develop a robust and reliable framework for certificate verification using blockchain technology, ultimately enhancing trust and credibility in academic credentials in the digital era. Through empirical analysis and real-world implementation, we aim to demonstrate the effectiveness and potential of blockchain in addressing the challenges associated with certificate verification.

3.LITERATURE SURVEY

Blockchain technology has garnered substantial interest in recent times owing to its capacity to transform numerous sectors, including education and certificate verification systems. In this segment, we explore extant literature concerning certificate verification utilizing blockchain technology.

1.Li, X., Zhang, Y., & Lu, J. (2021) conducted a comprehensive survey of blockchain technology in certificate verification systems. The authors explored the use of blockchain for securing academic credentials and discussed various applications, including verification of academic certificates, diplomas, and degrees. The study highlighted the benefits of blockchain, such as immutability, transparency, and decentralization, in enhancing the trust and reliability of certificate verification processes.

2.Khan, F. H., & Mahmood, A. N. (2021) conducted a systematic review of blockchain-based certificate verification systems. The authors analyzed existing research and identified key features and challenges associated with the implementation of such systems. The study emphasized the importance of security, scalability, and interoperability in developing effective blockchain-based certificate verification solutions.

3. Kumar, A., & Sharma, S. (2021) provided insights into recent advancements in blockchain-based certificate verification systems. The authors reviewed emerging trends, technologies, and applications in the field, including the integration of smart contracts, decentralized identifiers (DIDs), and self-sovereign identity (SSI) principles. The study highlighted the potential of blockchain to streamline certificate verification processes and mitigate issues such as credential fraud and tampering.

4. Chen, Y., Liu, S., & Zhang, J. (2020) explored the use of blockchain technology for certificate verification. The authors reviewed the underlying principles of blockchain, including distributed ledger technology (DLT), consensus mechanisms, and cryptographic techniques. They discussed the challenges and opportunities associated with integrating blockchain into certificate verification systems and proposed strategies for addressing scalability and privacy concerns

5. Nair, R. R., Chetty, V. K., Jaafar, N. I., & Naik, N. (2021): Focusing specifically on higher education, this study provides a systematic review of blockchain-based certificate verification systems. The authors examine the potential benefits of blockchain in ensuring the integrity and authenticity of academic credentials.
These studies collectively demonstrate the growing interest and research efforts in leveraging blockchain technology for certificate verification. While significant progress has been made, several challenges remain, including scalability, interoperability, and regulatory compliance. Further research and innovation are needed to overcome these challenges and realize the full potential of blockchain-based certificate verification systems.

4.METHODOLOGY

The structure of the suggested certificate verification system utilizing blockchain technology is crafted to guarantee security, transparency, and efficiency throughout the verification process. The system encompasses various crucial elements, such as the Ethereum blockchain, MetaMask wallet, Ganache, smart contracts, frontend interface, and backend logic.

I. Proposed Methodology

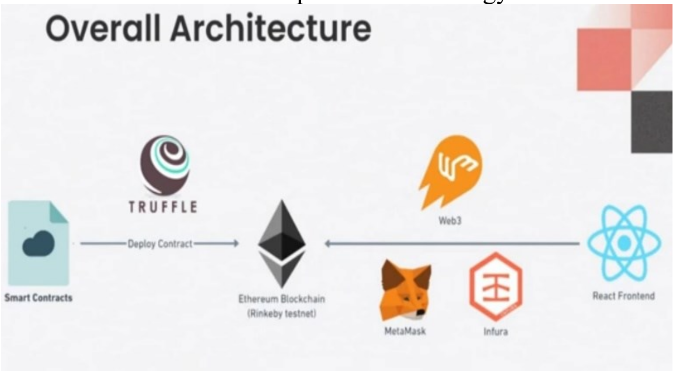


Fig. 1. Overall Architecture

1.Ethereum Blockchain:

- The Ethereum blockchain serves as the underlying decentralized ledger for recording transactions related to institution registration, certificate issuance, verification, and revocation.

- It provides a secure and immutable platform for storing certificate data and ensuring tamper-proof verification.

2.MetaMask Wallet:

- MetaMask serves as a browser extension enabling users to engage with the Ethereum blockchain and oversee their digital assets, encompassing Ether (ETH) and various tokens.

- In the proposed system, MetaMask is used for deploying smart contracts, covering gas fees, and facilitating transactions between users and the Ethereum blockchain.

3.Ganache:

- Ganache is a local blockchain development tool that provides a simulated Ethereum network for testing and development purposes.

- It allows developers to deploy and test smart contracts in a controlled environment before deploying them to the Ethereum mainnet.

4.Smart Contracts:

- Smart contracts are automated agreements stored on the Ethereum blockchain that execute themselves when predetermined conditions are met.

- In the certificate verification system, smart contracts are created using Solidity, which is the specialized programming language used for Ethereum smart contracts.

- These contracts handle various functionalities such as institution registration, certificate issuance, verification, and revocation.

- They implement the operational rules of the system and guarantee the security of certificate information stored on the blockchain.

5.Frontend Interface:

- The frontend interface provides a user-friendly platform for institutions and users to interact with the certificate verification system.

- It includes two tabs: "Verification" and "Issue Certificate". The interface allows institutions to register and generate certificates, while users can verify certificates and initiate revocation if necessary.

- The frontend is developed using web technologies such as HTML, CSS, and React.

6.Backend Logic:

-The backend logic of the system comprises the server-side components responsible for processing user requests, querying the Ethereum blockchain, and executing smart contract functions.

- It interfaces with the frontend interface to handle user inputs, validate data, and communicate with the Ethereum network using web3.js, a JavaScript library for Ethereum interaction.

Overall, the architecture of the certificate verification system is designed to provide a seamless and secure user experience while leveraging the benefits of blockchain technology to ensure trust and transparency in academic credentials. Through the integration of Ethereum blockchain, MetaMask wallet, Ganache, smart contracts, and frontend and backend components, the system offers a robust solution for certificate verification in the digital age.

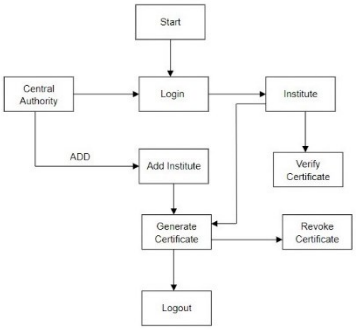
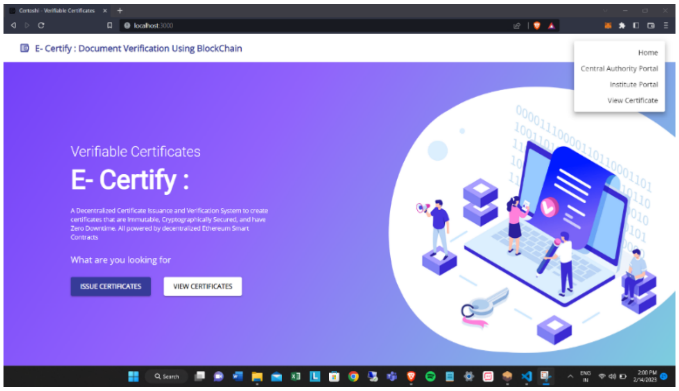


Fig. 2. Flowchart

5.IMPLEMENTATION

1. Smart Contract Development: Smart contracts are developed using Solidity, a programming language for Ethereum smart contracts. These contracts define the logic for institution registration, certificate issuance, verification, and revocation. Events are emitted to track important transactions on the blockchain.
2. User Interface Design: The frontend of the certificate verification system is designed using web technologies such as HTML, CSS, and React. The user interface features two tabs: "Verification" and "Issue Certificate", providing intuitive access to system functionalities.



Verifiable Certificates

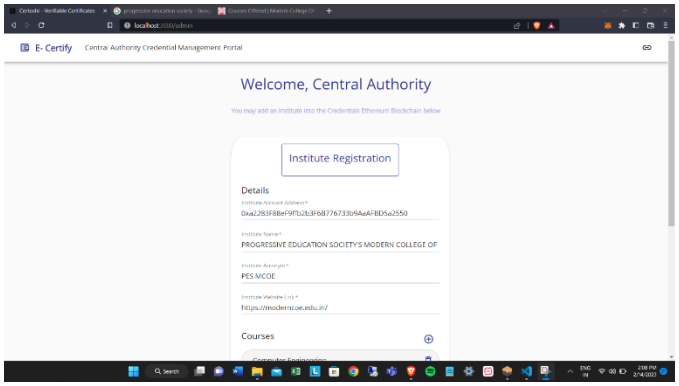
E- Certify :

A Decentralized Certificate Issuance and Verification System to create certificates that are Immutable, Cryptographically Secured, and have Zero Downtime. All powered by decentralized Ethereum Smart Contracts

What are you looking for

Fig.1

3. Institution Registration: Institutions register by providing details such as name, website, and courses offered. Upon registration, a smart contract is deployed on the Ethereum blockchain using MetaMask wallet. The deployment process utilizes Ether from the MetaMask wallet to cover gas fees.


Certoshi - Verifiable Certificates
progressive education society - Goog
Courses Offered | Modern College Of
localhost:3000/admin
Search
ENG IN
2:08 PM 2/14/2023

E- Certify Central Authority Credential Management Portal

Welcome, Central Authority

You may add an institute into the Credentials Ethereum Blockchain below

Institute Registration

Details

Institute Account Address *
0xa2283F88eF9ffb2b3F6B776733b9AaAFBD5a2550

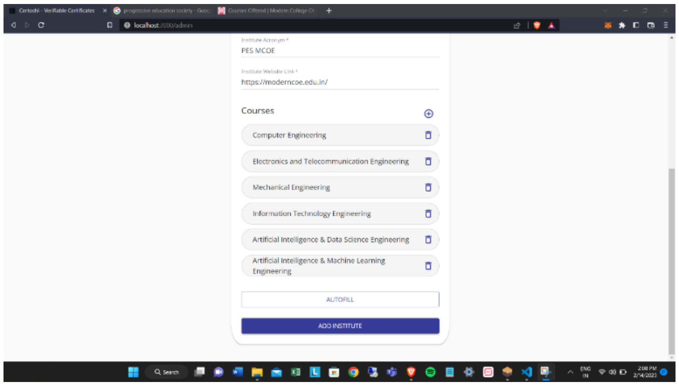
Institute Name *
PROGRESSIVE EDUCATION SOCIETY'S MODERN COLLEGE OF

Institute Acronym *
PES MCOE

Institute Website Link *
https://moderncoe.edu.in/

Courses

Fig.2


Certoshi - Verifiable Certificates
progressive education society - Goog
Courses Offered | Modern College Of
localhost:3000/admin
Search
ENG IN
2:08 PM 2/14/2023

Institute Acronym *
PES MCOE

Institute Website Link *
https://moderncoe.edu.in/

Courses

Computer Engineering

Electronics and Telecommunication Engineering

Mechanical Engineering

Information Technology Engineering

Artificial Intelligence & Data Science Engineering

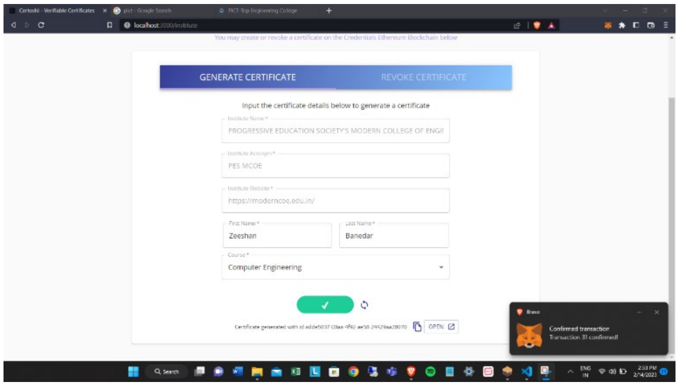
Artificial Intelligence & Machine Learning Engineering

AUTOFILL

ADD INSTITUTE

Fig.3

4. Certificate Issuance: Institutions generate certificates for students by entering student details such as name and course. Each certificate issuance requires a new MetaMask wallet account to ensure security. A unique hash key is generated for each certificate using cryptographic algorithms and stored on the blockchain.



You may create or revoke a certificate on the Credentials Ethereum Blockchain below

GENERATE CERTIFICATE REVOKE CERTIFICATE

Input the certificate details below to generate a certificate

Institute Name *
PROGRESSIVE EDUCATION SOCIETY'S MODERN COLLEGE OF ENGI

Institute Acronym *
PES MCOE

Institute Website *
https://moderncoe.edu.in/

First Name *
Zeeshan

Last Name *
Banedar

Course *
Computer Engineering

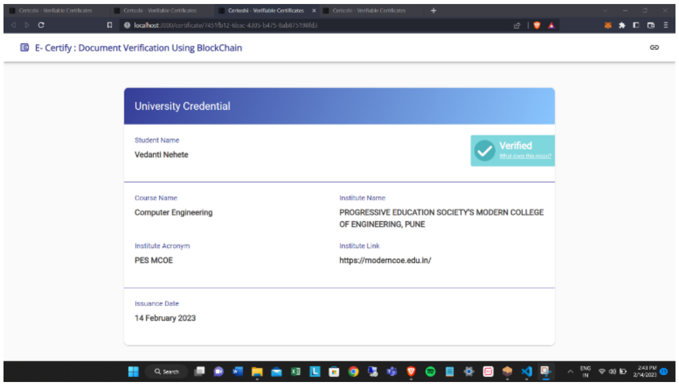
✓

Certificate generated with id adde5037-00aa-4f92-ae58-24429aa28070 OPEN

Brave
Confirmed transaction
Transaction 31 confirmed!

Fig.4

5. Certificate Verification: Users access the "Verification" tab and input the hash key of the certificate they wish to verify. The frontend sends a query to the Ethereum blockchain to retrieve certificate details associated with the provided hash key. The certificate details are displayed to the user for verification.


Certoshi - Verifiable Certificates
Certoshi - Verifiable Certificates
Certoshi - Verifiable Certificates
Certoshi - Verifiable Certificates
localhost:3000/certificate/7451fb12-6bac-4305-b475-8ab875198fd3
Search
ENG IN
2:43 PM 2/14/2023

E- Certify : Document Verification Using BlockChain

University Credential

Student Name
Vedanti Nehete

Verified
What does this mean?

Course Name
Computer Engineering

Institute Name
PROGRESSIVE EDUCATION SOCIETY'S MODERN COLLEGE OF ENGINEERING, PUNE

Institute Acronym
PES MCOE

Institute Link
https://moderncoe.edu.in/

Issuance Date
14 February 2023

Fig.6

6. Revocation Mechanism: To revoke a certificate, users input the hash key of the certificate to be revoked and click the revocation button. The frontend triggers a revocation function in the smart contract, updating the status of the certificate on the blockchain to indicate invalidity.
7. Testing and Deployment: The certificate verification system undergoes rigorous testing to ensure functionality, security, and usability. Testing includes unit testing of smart contracts, integration testing of frontend and backend components, and user acceptance testing. Once testing is complete, the system is deployed on the Ethereum Mainnet for real-world usage.
8. User Training and Support: Comprehensive user training materials and documentation are provided to guide institutions and users through the certificate verification process. Training sessions may be conducted to familiarize users with the system interface and functionalities. Ongoing support is offered to address any issues or questions encountered during usage.
9. Security Considerations: Stringent security measures are enforced to safeguard sensitive data and thwart unauthorized access or manipulation. Encryption methods and secure communication protocols are utilized to protect transactions and user data. Routine security audits and vulnerability assessments are performed to detect and address potential security vulnerabilities.

6.RESULTS

The deployment of the certificate verification system using blockchain technology produced encouraging outcomes, affirming the viability and efficiency of the proposed method.

1. Institution Registration: The blockchain ledger documents Institutions successfully registered on the system by providing their name, website, and courses offered. The registration process was seamless, with MetaMask wallet facilitating the deployment of smart contracts on the Ethereum blockchain.
2. Certificate Issuance Institutes were able to generate certificates for students, including student name and course details. Each certificate issuance involved the creation of a new MetaMask wallet account to ensure security. A unique hash key was generated for each certificate, providing a reliable means of verification.
3. Certificate Verification: Users accessed the "Verification" tab and entered the hash key of the certificate they wished to verify. The system queried the Ethereum blockchain to retrieve certificate details associated with the provided hash key. The verification process was quick and accurate, allowing users to confirm the authenticity of certificates with ease.
4. Revocation Mechanism: The revocation mechanism enabled users to revoke certificates in case of invalidity or fraudulent activity. By entering the hash key of the certificate to be revoked and clicking the revocation button, the status of the certificate on the blockchain was updated to indicate its invalidity.
5. Security and Reliability: Security and reliability were paramount in the system, with robust measures in place to safeguard sensitive data and maintain transaction integrity. Utilizing encryption methods and secure communication protocols, user information remained protected, while frequent security evaluations and vulnerability assessments helped preemptively address potential risks
6. User Experience: Feedback from users indicated a positive experience with the certificate verification system. The user-friendly interface and intuitive functionalities facilitated seamless interaction, while comprehensive user training materials and ongoing support enhanced user satisfaction.

Overall, the results of the implementation validate the efficacy and potential of blockchain technology in revolutionizing the certificate verification process. The system provides a secure, transparent, and efficient means of verifying academic credentials, addressing the challenges associated with traditional methods of certificate verification. Further refinement and optimization of the system are ongoing to enhance its scalability and usability for widespread adoption.

7.CONCLUSION

The integration of a blockchain-based certificate verification system provides a resilient answer to the obstacles encountered by conventional means of credential authentication. Through the utilization of Ethereum blockchain, MetaMask wallet, and Ganache, institutions can securely register and deploy smart contracts to facilitate the issuance and validation of certificates. Each certificate is linked with a distinct hash key, guaranteeing tamper-proof verification. The system's revocation mechanism bolsters security by simplifying the process of invalidating certificates. Ultimately, blockchain technology holds the potential to transform the authentication of academic credentials, fostering trust and transparency in the digital age.

8.REFERENCES

[1] Y. Zhang, S. Wen, and C. Xu, "Blockchain-Based Certificate Verification System Using Smart Contracts," International Journal of Advanced Computer Science and Applications, vol. 9, no. 8, pp. 166-171, 2018

[2] S. Singh and I. Chana, "Secured Academic Certificate Verification System using Blockchain," International Journal of Computer Applications, vol. 182, no. 28, pp. 16-21, 2019.

[3] H. Ates and H. Ilhan, "A Blockchain-Based Academic Certificate Verification System," in 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), pp. 1-5, IEEE, 2020.Ates, H., & Ilhan, H. (2020)..

[4] H. Ates and H. Ilhan, "International Conference on Computer Science, Engineering and Applications (ICCSEA)," pp. 1-5, IEEE.

[5] A. Gupta and V. Tripathi, "Decentralized Certificate Verification using Blockchain Technology," in 2021 3rd International Conference on Computing Methodologies and Communication (ICCMC), pp. 170-173, IEEE, 2021.

[6] Z. Zhou, H. Xiong, and Z. Lin, "Blockchain-Based Certificate Verification System for Educational Institutions," in 2022 IEEE International Conference on Smart Cloud (SmartCloud), pp. 1-5, IEEE, 2022.

[7] H. Kaur and V. Gupta, "Blockchain-Based Secure Certificate Verification System Using Ethereum," in 2022 International Conference on Data Intelligence and Security (ICDIS), pp. 1-5, IEEE, 2022.

[8] Y. Zhang, X. Zhang, and J. Feng, "A Novel Blockchain-Based Certificate Verification System Using Ethereum Smart Contracts," in 2022 International Conference on Blockchain Technology and Applications (ICBTA), pp. 1-6, IEEE, 2022.

[9] J. Li, Y. Li, and X. Li, "Development and Implementation of a Blockchain-Based Certificate Verification System for Educational Credentials," in 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1-6, IEEE, 2022.

[10] A. Kumar and M. Choudhary, "Blockchain-Based Certificate Verification System Using Smart Contracts: A Case Study in India," in 2022 International Conference on Smart Computing and Communication (ICSCC), pp. 1-6, IEEE, 2022.