INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

Blockchain based Certificate Generation and Validation

Omraj Jadhav, Akhilesh Dange, Pransenjit Bhosale, Aniket Chanvan, Yashshri Deshmukh,

Akshanta Dhumal, Dr. Shabina Modi

U.G. Student, Department of Computer Engineering, Karmaveer Bhaurao Patil College of Engineering, Satara,

Maharashtra, India

Associate Professor, Department of Computer Engineering, Karmaveer Bhaurao Patil College of Engineering, Satara,

Maharashtra, India

ABSTRACT: This paper proposes a blockchain-based digital certificate system to tackle the issue of fraudulent educational certificates. Traditional certificate issuance and verification methods lack transparency and are susceptible to counterfeiting, damaging credibility. The proposed system leverages blockchain's immutability to issue verifiable, anti-counterfeit digital certificates. Electronic certificate files are generated, and their hash values are stored on the blockchain, with unique QR codes or URLs for authentication. Users store certificates in Ethereum blockchain digital lockers using smart contracts.

Organizations verify certificates by cross-checking provided QR codes or URLs against blockchain data. All transactions are recorded on the blockchain, ensuring transparency. The system reduces certificate forgery risks through automated, open processes. It offers a reliable, user-friendly solution for educational institutions, employers, and individuals, enhancing certificate management integrity while minimizing risks associated with fraudulent credentials.

KEYWORDS: Blockchain, Ethereum, Smart Contracts, Security, Certificate Generation.

I. INTRODUCTION

Document verification is a challenging process fraught with obstacles and time-consuming procedures, as indicated by statistics from the Indian Ministry of Education. Instances of forged graduation certificates are frequently encountered due to insufficient anti-forgery measures. To address this issue of counterfeit certificates, we propose implementing a digital certificate system based on blockchain technology. Educational institutions issue certificates as the most significant documents to their students. However, the lack of transparency and verifiability in the issuance process makes it relatively easy to create counterfeit certifications that can be difficult to detect and may even appear identical to genuine ones. Document forgery damages the credibility of the issuing entity and the document holder. Our objective is to establish a blockchain-based digital certificate system to tackle the problem of certificate forgeries, leveraging the immutability of blockchain technology to issue digital certificates with embedded verifiability and anti-counterfeit features.

II. LITERATURE REVIEW

Blockchain technology is revolutionizing the management of digital certificates by addressing key issues of forgery, transparency, and revocation. Traditional systems often fall short in preventing certificate fraud due to weak anti-counterfeit measures, leading to frequent instances of forgery. Blockchain's immutable nature enables the creation of tamper-proof digital certificates, with QR codes and hash values stored on the blockchain for easy and secure verification. This system enhances the reliability and authenticity of certificates, making it difficult for counterfeit ones to go undetected. Moreover, blockchain facilitates certificate transparency and revocation by recording the issuance and status of certificates on a public ledger, ensuring that only valid and officially issued certificates are recognized. This approach improves the security of web communications, particularly through protocols like SSL/TLS, by ensuring that public keys are distributed securely. Various implementations, such as those utilizing IBM's Hyperledger Fabric and consortium blockchains, demonstrate the practicality and effectiveness of these solutions. They provide a decentralized, collaborative framework for managing certificate revocation lists (CRLs) across multiple certification authorities (CAs), enhancing trust, access reliability, and data synchronization. This

innovative use of blockchain technology not only safeguards against fraudulent certificates but also expands the potential applications of digital certificates in various sectors.

III. METHODOLOGY

The proposed system involves the following steps:

1. Issuing User Certificates: Users can obtain their certificates from colleges or government agencies through the Ethereum network.
2. Digital Lockers and Blockchain Storage: Each user has a secure digital locker on the Ethereum blockchain, where they can store their certificates using smart contracts, ensuring immutability and security.
3. Unique Certificate Identifier: Every certificate is assigned a distinct hash number for safe identification.
4. Generate Unique URL/QR Code: An automatically generated unique URL or QR code is linked to each blockchain-stored certificate.
5. Share Certificates: Users share the generated QR code or URL with organizations or entities requesting verification.
6. Organization Verification: Organizations initiate the verification process by visiting the website and providing the URL or QR code obtained from the user.
7. Validation: The system authenticates certificates by verifying the blockchain data associated with the provided URL or QR code, ensuring legitimacy.
8. Record Keeping and Inspection: All certificate-related transactions, including issuance and validation, are recorded on the Ethereum blockchain, maintaining transparency and security.
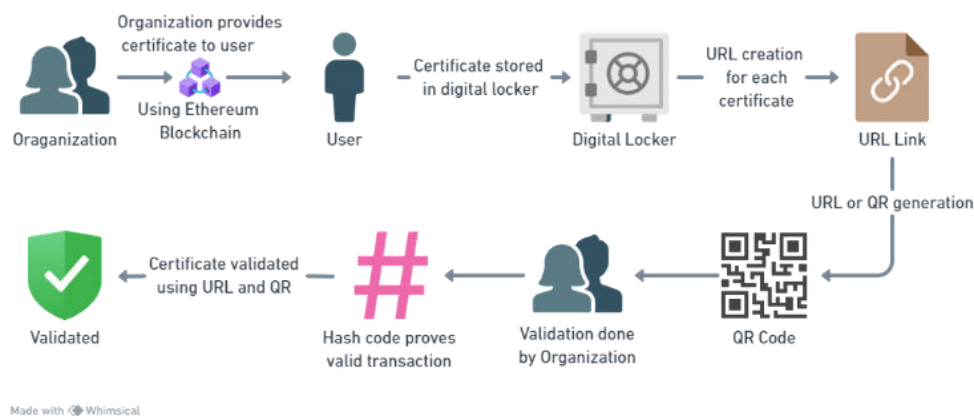
IV. PRELIMINARY DATA

A. Existing System:
Traditional certificate issuance and verification processes often lack robust anti-forgery measures, enabling the creation of counterfeit documents.

B. Proposed System:
The proposed blockchain-based solution aims to reduce the possibility of certificate forgery. The automated certificate issuance and application processes ensure transparency and openness, allowing organizations or entities to verify the authenticity of certificates through the system.

C. Advantages of proposed system:
The possibility of certificate forgery is decreased by the suggested blockchain-based solution. The automated certificate issue process in the system is open and transparent, as is the certificate application process.

FUNCTIONAL REQUIREMENTS:
- Modeling
- Data preprocessing
- Prediction
- Data collection

- Training and testing

NON-FUNCTIONAL REQUIREMENTS:

Non-functional requirements (NFRs) outline a software system's quality attributes. They evaluate the software system based on non-functional criteria like usability, security, portability, and responsiveness that are essential to its success. An example of a nonfunctional need might be "how quickly can I load the website?" Systems that don't fulfill user demands might be the consequence of not meeting non-functional criteria.

- Scalability
- Availability
- Usability
- Capacity
- Interoperability
- Security
- Environmental
- Reliability
- Manageability
- Recoverability
- Serviceability
- Data integrity

V. DISCUSSION

A. Blockchain Technology:

Blockchain is a decentralized, immutable ledger that offers potential for various applications. It consists of a distributed database where multiple users can add, modify, and remove entries, but once data is input, it cannot be altered or removed. Hashing is a crucial aspect of blockchain technology, where a message digest or hash value is generated from a text string, ensuring data integrity during transmission.

B. Smart Contracts:

Self-executing contracts, known as smart contracts, explicitly incorporate the terms of an agreement into the code. Running on blockchain platforms like Ethereum, smart contracts automatically execute and enforce the terms once predefined conditions are met, revolutionizing industries like finance, supply chain management, and legal procedures due to their tamper-proof, secure, and decentralized nature

C. Advantages of Proposed System:

- Modern and relevant: Aligns with contemporary digital practices.
- Certificates cannot be altered: Ensures authenticity once stored on the blockchain.
- Cost savings: Reduces resources required for paperwork and manual checks.
- Faster certificate issuance: Enables direct issuance on the blockchain.
- Transparency and trust: Secure records maintain accountability.
- Easy verification: Individuals can quickly verify certificates using URLs or QR codes.
- Reliable validation: Provides a uniform and reliable method for certificate verification.
- User-friendly: Designed for ease of use by both credential holders and verifiers.
- Better security: Utilizes the highly secure and nearly impossible-to-hack blockchain technology.

D. Statement of Limitation:

- Internet dependency: The system requires internet connectivity for distribution and verification.
- Initial setup complexity: The setup, smart contract development, and system integration can be challenging and time-consuming.

VI. IMPLEMENTATION

The proposed system aims to prevent certificate forgery by introducing a blockchain-based certificate verification method. It consists of three modules:

A. Company Module:

- A company user needs to register and log in to the system.
- They can then upload a certificate for verification.

- The system compares the digital signature of the uploaded certificate with the signatures stored in the Blockchain.
- If the digital signature matches the original certificate, the authentication is successful.

B. Admin Module:
- The admin, acting as an educational authority, logs in with the username "admin" and password "admin."
- Upon login, the admin uploads the student's information and certificate to the blockchain.
- Each certificate is assigned a unique hash code that serves as a digital signature.
- The hash code is used to generate a QR code linked to the student's certificate.
- Scanning the QR code with a smartphone allows retrieval of information from the blockchain.
- If the QR code is found in the blockchain, it confirms the successful validation of the certificate.

C. Scanner Module:
- Educational institutions and companies will maintain this stand-alone module.
- Users can scan a QR code to retrieve information from the blockchain.

The implementation process is as follows:
1. Run the run.bat file to start the Python server.

2. Open a web browser and navigate to http://127.0.0.1:5000/index.
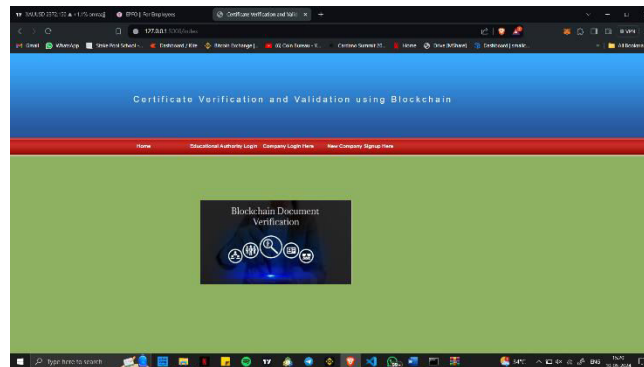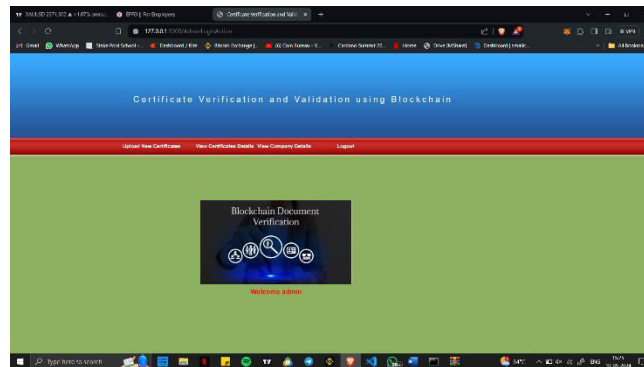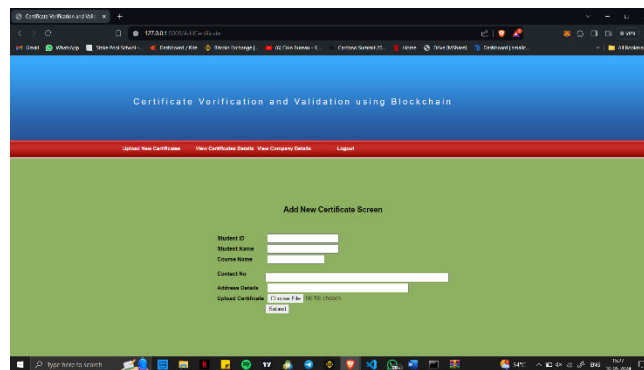

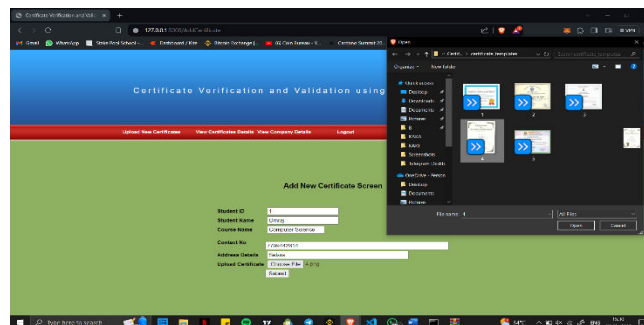3. Click the "Educational Authority Login" link to access the admin login page.
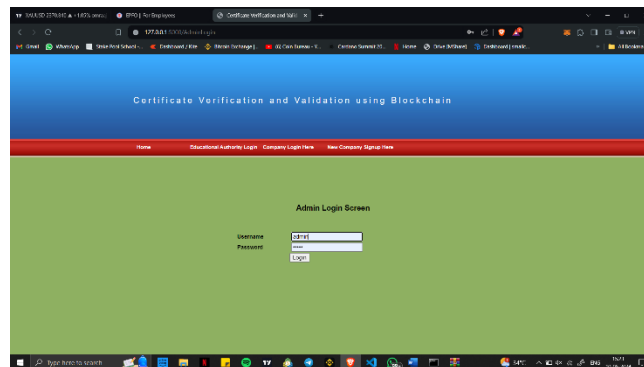
4. After logging in as an admin, you can upload new certificates by providing student information and the certificate file.
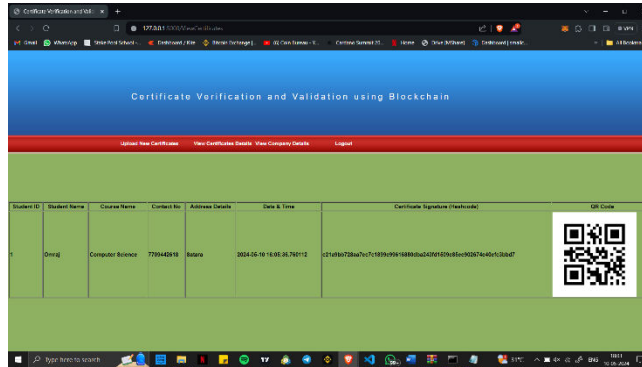

5. The system will generate a digital signature and a QR code image for each uploaded certificate.
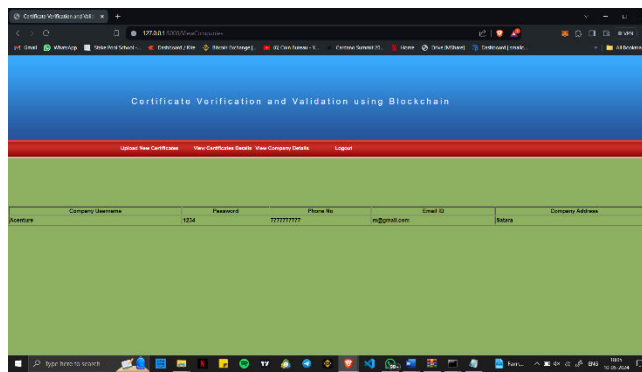

6. Admins can view registered companies and their details.
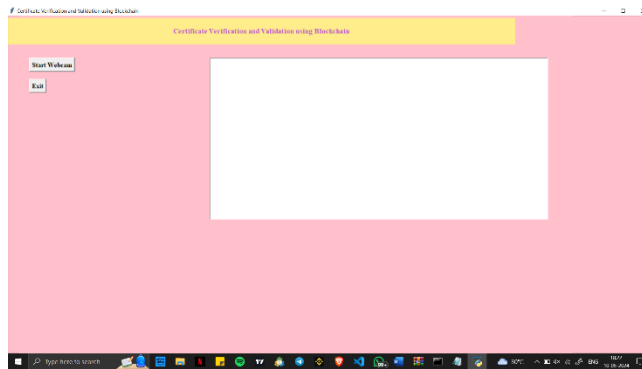

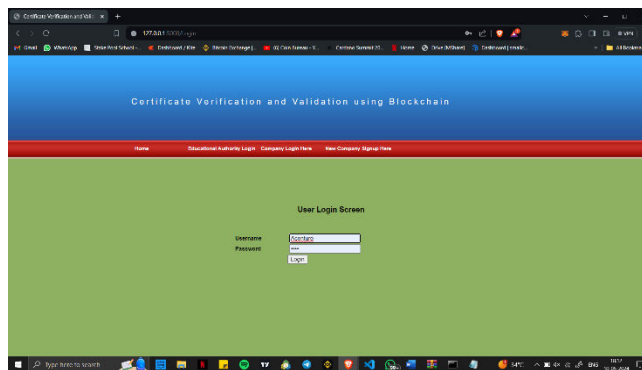7. Companies can register themselves and log in to the system.

8. Companies can upload a copy of the student's certificate and initiate the verification process.
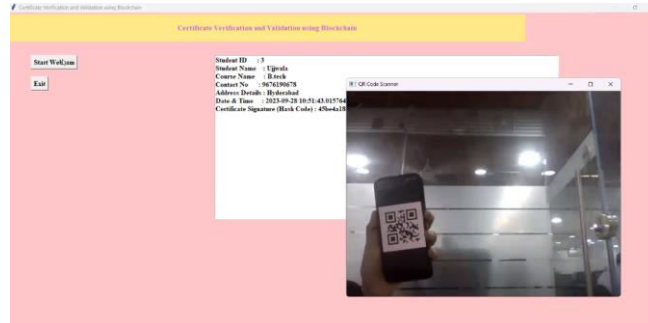

9. The system will display the verification result, indicating whether the certificate is authentic or not.

10. To validate certificates using QR codes, run the RunWebCam.bat file.

11. Click "Start Webcam" to activate the camera.

12. Scan the QR code, and the system will retrieve and display the corresponding certificate information from the Blockchain.

The implementation section provides a step-by-step guide to using the blockchain-based certificate verification system, including the roles and functionalities of the admin, company, and scanner modules.

VII. CONCLUSION

The proposed blockchain-based method significantly reduces the likelihood of certificate forgery. The system's automated certificate issuance and application processes ensure transparency and openness, allowing companies or groups to verify the authenticity of any certificate. The information is accurate and secure, thanks to the immutable and decentralized nature of blockchain technology. Potential future work could explore further enhancements, such as integrating additional security measures or expanding the system to other domains beyond educational certificates.

REFERENCES

[1] "Blockchain Technology: Principles and Applications" by Marc Pilkington, which is a part of the Research Handbook on Digital Transformations edited by F. Xavier Olleros and Majlinda Zhegu, the author gives a detailed overview of blockchain technology and its applications. This includes conversations on certificate creation and validation.

[2] "Blockchain in Education: Introduction and Critical Review of the State of the Art" by Alexander Grech and Andréia Inamorato dos Santos, published in Publications, MDPI. This paper explores diverse applications of blockchain technology in education, encompassing certificate issuance and verification among others.

[3] "Towards Blockchain-based Digital Certificates for Learning: Technical Issues and Future Directions" by H. Drechsler, D. Bogers, M. Vuorikari, and S. Kalz, published in the International Journal of Educational Technology in Higher Education, the authors delve into the technical aspects and hurdles involved in deploying blockchain-based digital certificates within the realm of learning.

[4] "Blockcerts: An Open Infrastructure for Academic Credentials on the Blockchain" authored by M. Sporny, D. Longley, and M. Allen, appears in IEEE Security & Privacy. This paper introduces Blockcerts, an open standard designed for blockchain-based digital certificates, detailing its implementation and exploring potential applications.

[5] "Blockchain Solutions for Credentials and Certificates: Examples and Challenges from the European Perspective" by Pauline van Mourik, published in European Journal of Education. This paper discusses examples of blockchain solutions for credentials and certificates in Europe and examines the challenges associated with their implementation.

[6] "Designing Blockchain-Based Systems for Secure and Trustworthy Credentials" published in IEEE Transactions on Dependable and Secure Computing by K. Ren, A. Yu, X. Wang, and W. Lou. The architecture for developing blockchain-based systems for reliable and safe credentials, that involve certificate creation and validation, is presented in this paper.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING