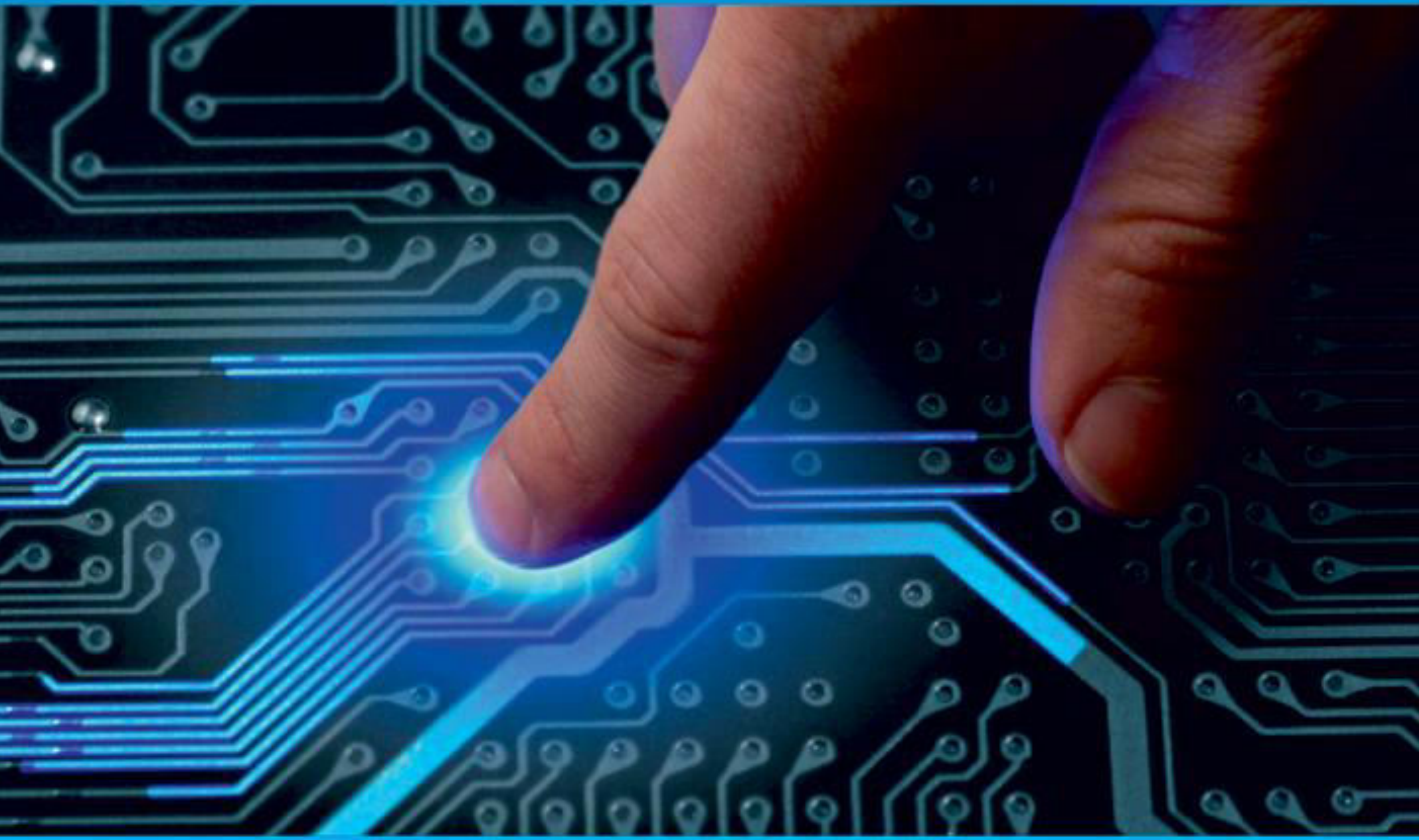
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203159 |

Certificate Verification and Validation Using Block Chain

[1] Ravikanti Shreya, [2] Mohammad Sameer, [3] Dymakka Himavarsha, [4] T. Veda Reddy

[1, 2, 3.] Students, Department of Computer Science and Engineering, Anurag University, Hyderabad, Telangana, India

[4.] Associate professor, Department of Computer Science and Engineering & Anurag University, Hyderabad, Telangana, India

ABSTRACT: Certificate forgery is a long-standing problem that plagues various industries, including education, professional certifications, and legal documentation. Due to the lack of an effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed. To solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. For students, educational certificates are the most important documents issued by their universities. However, as the issuing process is not that transparent and verifiable, fake certificates can be easily created. A skillful generated fake certificate is always hard to detect and can be treated as the original. With the increase of forged documents, the credibility of both the document holder and the issuing authority is jeopardized. To solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. By the modifiable property of blockchain, the digital certificate with anti-counterfeit and verifiability could be made. The proposed system leverages the capabilities of blockchain technology to create a robust, decentralized, and tamper-resistant certificate verification platform. Blockchain technology offers a decentralized and immutable way of storing and managing data, making it an ideal candidate for revolutionizing certificate verification. By leveraging blockchain, the entire process becomes more efficient and secure. Each certificate issuance is recorded in a tamper-proof manner with a timestamp, making it virtually impossible to alter or delete the information. Furthermore, the decentralized nature of blockchain eliminates the reliance on a central authority, reducing the risk of data manipulation and building trust in the verification process. Finally, the proposed system revolutionizes the current practices and address the challenges associated with certificate forgery, offering a more secure, efficient, and trustworthy solution.

KEYWORDS: Certificate forgery, Blockchain, Digital Certificate, Verification, Decentralized, Tamper-resistant, Immutable, Trustworthy.

I. INTRODUCTION

An estimated 26.3 million students enrolled in Indian higher education in 2018-19 and nearly 9 million graduates annually. For admission, students need to produce these certificates in institutions or companies. Tracking these certificates and validating their authenticity manually becomes a tedious job. The absence of an appropriate anti-forge system leads to a scenario where it is found that the graduation certificate is forged. To make the data more secure and safe, everything needs to be digitalized with the principle of Confidentiality, Reliability, and Availability. All of these can be achieved with a technology named Blockchain. Briefly, the flow of our system will consist of a Certificate issuer who will generate certificates and those certificates will be validated by a panel within that organization before being sent to a student. Each certificate will have a unique hash key which can be used to validate the authenticity of the certificate by any organization through the portal. The benefit of such a system is that the student also faces less risk of losing or damaging a certificate and the validation of the certificate can also be done quite easily. The proposed system leverages the capabilities of blockchain technology to create a robust, decentralized, and tamper-resistant certificate verification platform. Blockchain technology offers a decentralized and immutable way of storing and managing data, making it an ideal candidate for revolutionizing certificate verification. By leveraging blockchain, the entire process becomes more efficient and secure. Each certificate issuance is recorded in a tamper-proof manner with a timestamp, making it virtually impossible to alter or delete the information. Furthermore, the decentralized nature of blockchain eliminates the reliance on a central authority, reducing the risk of data manipulation and building trust in the verification process.

II. RELATED WORK

Various research endeavours in the realm of certificate validation and verification harness a multitude of methodologies tailored for analysing and ensuring the authenticity of certificates through blockchain technology. OpenCerts is an open-source framework developed by the Government Technology Agency (GovTech) of Singapore for issuing and verifying tamper-resistant digital certificates on the Ethereum blockchain. It allows educational institutions and organizations to issue verifiable certificates that can be easily verified by employers, educational institutions, and other stakeholders. The Accord Project is an open-source initiative focused on developing smart legal contracts and legal automation solutions using blockchain technology. It includes projects such as the Legal Blockchain Consortium, which explores the use of blockchain for verifying and validating legal documents, including certificates, contracts, and agreements. Certifaction is a blockchain-based platform for issuing and verifying certificates and diplomas. It allows institutions to issue digital certificates that are stored on the Ethereum blockchain, providing a secure and tamper-proof record of achievement. Individuals can easily verify the authenticity of their certificates using the Certifaction platform.

III. EXISTING METHOD

In the existing systems, Hyperledger is an open-source blockchain framework renowned for its versatility and applicability in enterprise environments. With its modular architecture and diverse range of tools like Hyperledger Fabric and Hyperledger Sawtooth, organizations can build tailored blockchain networks to suit their specific needs. However, it's important to acknowledge certain limitations. Lastly, interoperability with other blockchain platforms or legacy systems can pose challenges, hindering seamless integration.

Drawbacks of Existing Systems

The drawbacks of the current system include the following:

- Scalability can become a concern as network size increases, potentially impacting performance.
- The complexity of setup and maintenance demands specialized knowledge, leading to higher implementation costs.
- Privacy concerns may arise due to the permissioned nature of Hyperledger networks, raising questions about data confidentiality.
- Lastly, interoperability with other blockchain platforms or legacy systems can pose challenges, hindering seamless integration.

IV. PROPOSED METHOD

This proposed method aims to leverage Python's flexibility and Ethereum's decentralized infrastructure to establish a secure and transparent system for certificate verification. It provides:

- **Decentralization**: By integrating with the Ethereum blockchain, the certificate verification process becomes decentralized, eliminating the need for a central authority.
- **Immutable Record-Keeping**: Ethereum blockchain ensures that once certificate data is recorded, it cannot be altered or tampered with, providing a tamper-proof record of certificate issuance and verification activities.
- **Enhanced Security**: Utilizing Ethereum's cryptographic techniques, certificate data can be securely hashed and stored on the blockchain, protecting it from unauthorized access or modification.
- **Transparency and Accountability**: Python scripts interacting with the Ethereum blockchain can provide transparent access to certificate records for all stakeholders, promoting accountability and trust in the verification process.

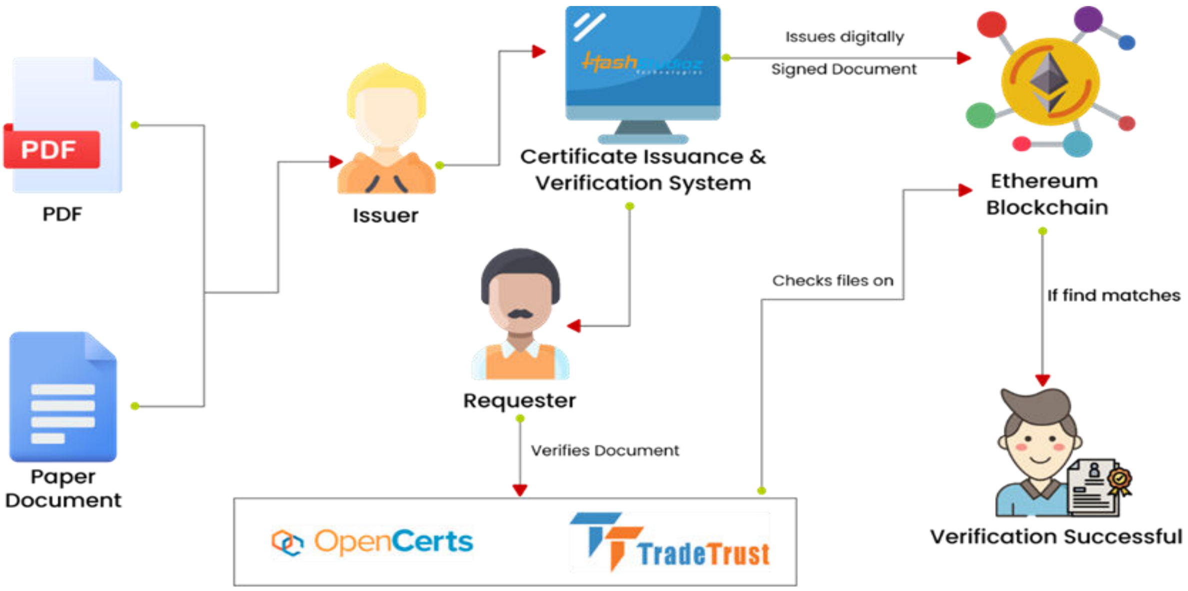


Fig 1: Flow Chart

V. SIMULATION RESULTS

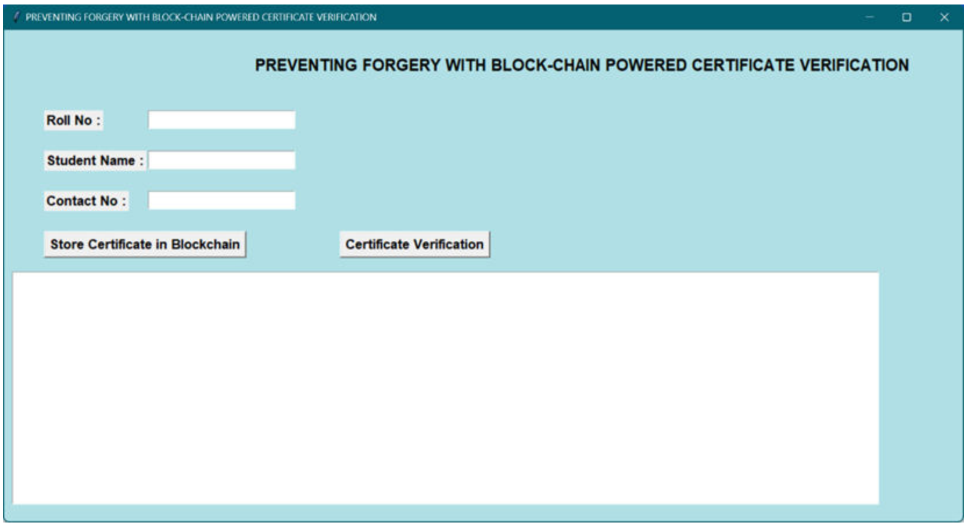
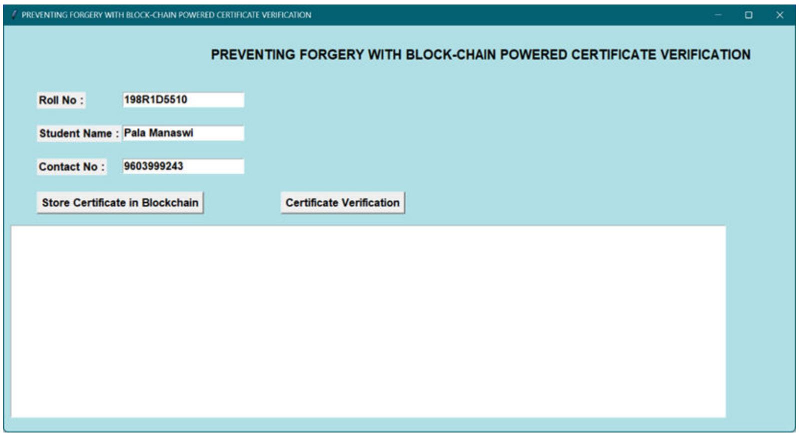

PREVENTING FORGERY WITH BLOCK-CHAIN POWERED CERTIFICATE VERIFICATION
PREVENTING FORGERY WITH BLOCK-CHAIN POWERED CERTIFICATE VERIFICATION
Roll No :
Student Name :
Contact No :
Store Certificate in Blockchain
Certificate Verification

Fig 2: Main GUI application of proposed blockchain powered certificate verification for forgery prevention.

Figure 2 shows the initial state of the graphical user interface (GUI) when the application is launched. It includes the following elements:

1. Title: "PREVENTING FORGERY WITH BLOCK-CHAIN POWERED CERTIFICATE VERIFICATION"
2. Buttons: "Store Certificate in Blockchain" and "Certificate Verification"
3. Entry fields for student details (Roll Number, Student Name, Contact Information)
4. A text widget for displaying information and results.
5. The main window with a specific size and background color (powder blue)

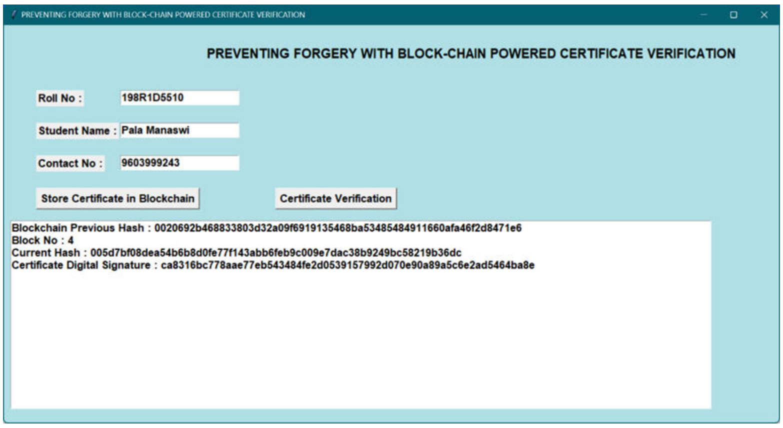

PREVENTING FORGERY WITH BLOCK-CHAIN POWERED CERTIFICATE VERIFICATION
PREVENTING FORGERY WITH BLOCK-CHAIN POWERED CERTIFICATE VERIFICATION
Store Certificate in Blockchain
Certificate Verification

Roll No : 198R1D5510

Student Name : Pala Manaswi

Contact No : 9603999243

Fig 3: GUI application after entering the details of student with roll number, student name, and contact information.


PREVENTING FORGERY WITH BLOCK-CHAIN POWERED CERTIFICATE VERIFICATION
PREVENTING FORGERY WITH BLOCK-CHAIN POWERED CERTIFICATE VERIFICATION
Store Certificate in Blockchain
Certificate Verification

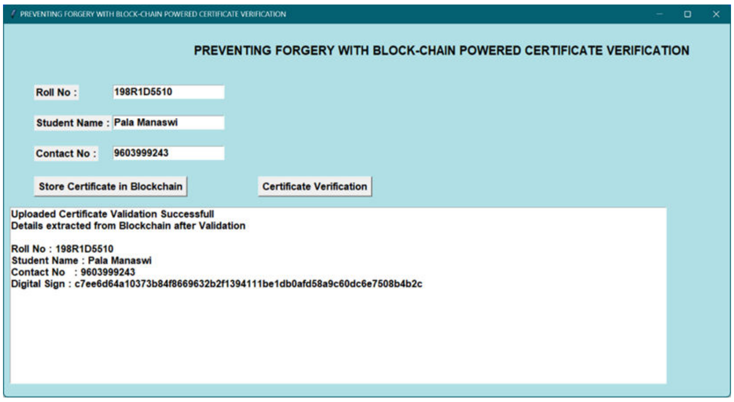
Roll No : 198R1D5510

Student Name : Pala Manaswi

Contact No : 9603999243

```
Blockchain Previous Hash : 0020692b468833803d32a09f6919135468ba53485484911660afa46f2d8471e6
Block No : 4
Current Hash : 005d7bf08dea54b6b8d0fe77f143abb6feb9c009e7dac38b9249bc58219b36dc
Certificate Digital Signature : ca8316bc778aae77eb543484fe2d0539157992d070e90a89a5c6e2ad5464ba8e
```

Fig 4: Illustration of proposed GUI application after storing the certificate with student entry details.


PREVENTING FORGERY WITH BLOCK-CHAIN POWERED CERTIFICATE VERIFICATION
PREVENTING FORGERY WITH BLOCK-CHAIN POWERED CERTIFICATE VERIFICATION
Store Certificate in Blockchain
Certificate Verification

Roll No : 198R1D5510

Student Name : Pala Manaswi

Contact No : 9603999243

```
Uploaded Certificate Validation Successfull
Details extracted from Blockchain after Validation

Roll No : 198R1D5510
Student Name : Pala Manaswi
Contact No   : 9603999243
Digital Sign : c7ee6d64a10373b84f8669632b2f1394111be1db0afd58a9c60dc6e7508b4b2c
```

Fig 5: Checking the certificate verification with test template as input and displaying the validation is successfully verified with student enrolment.

VI. CONCLUSION AND FUTURE WORK

In conclusion, the implementation of blockchain technology in certificate verification holds immense potential for combating the persistent problem of certificate forgery across various industries. By offering a decentralized, tamper-resistant, and transparent platform, this innovative approach addresses the limitations of traditional verification methods. The immutability of blockchain ensures that certificate records remain secure and unalterable, thereby enhancing their credibility and authenticity. Additionally, the elimination of central authorities reduces the risk of data manipulation and fosters trust in the verification process. However, to fully realize the benefits of blockchain-powered certificate verification, several challenges must be overcome. These include ensuring widespread adoption of the technology, addressing scalability issues, and developing user-friendly interfaces for individuals and institutions.

In future, we would like to enhance the application by adding following features:

- Implement QR code scanning for instant verification, eliminating manual entry of serial numbers and encryption keys.
- Introduce a configuration panel allowing universities to customize application settings according to their operational preferences.
- Develop a configuration panel similar to the university application, enabling customization and streamlined management.

REFERENCES

[1]. Almadani, M.S.; Alotaibi, S.; Alsobhi, H.; Hussain, O.K.; Hussain, F.K. Blockchain-based multi-factor authentication: A systematic literature review. Internet Things 2023, 23, 100844.

[2]. Kumar, P.; Kumar, R.; Gupta, G.P.; Tripathi, R.; Jolfaei, A.; Islam, A.N. A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. J. Parallel Distrib. Comput. 2023, 172, 69–83.

[3]. Sharma, P.C.; Mahmood, R.; Raja, H.; Yadav, N.S.; Gupta, B.B.; Arya, V. Secure authentication and privacy-preserving blockchain for industrial internet of things. Comput. Electr. Eng. 2023, 108, 108703.

[4]. Bordel, B.; Alcarria, R.; Robles, T. A Blockchain Ledger for Securing Isolated Ambient Intelligence Deployments Using Reputation and Information Theory Metrics; Wireless Networks: New York, NY, USA, 2023; pp. 1–7.

[5]. Selvarajan, S.; Srivastava, G.; Khadidos, A.O.; Khadidos, A.O.; Baza, M.; Alshehri, A.; Lin, J.C.-W. An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems. J. Cloud Comput. 2023, 12, 38.

[6]. Yazdinejad, A.; Parizi, R.M.; Dehghantanha, A.; Choo, K.-K.R. P4-to-blockchain: A secure blockchain-enabled packet parser for software defined networking. Comput. Secur. 2020, 88, 101629.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING