E – CERTIFICATE VALIDATION USING BLOCKCHAIN

Mahamkali Vishnu Teja[1], Meka Sharon Raju[2], Pabbisetty Poorna Sainth[3], Pasupuleti Bhanu Chaitanya[4]

[1,2,3,4] *UG Students, Department of CSE (IoT, Cybersecurity Including Blockchain Technology), Vasireddy Venkatadri Institute of Technology, Andhra Pradesh, India*

ABSTRACT

Traditional educational credential verification methods are vulnerable to forgery and require time-consuming manual processes. This project proposes a novel and secure E-certificate validation system leveraging blockchain technology. The system offers a secure, transparent, and efficient solution for all stakeholders: students, issuing institutions, and verifying companies. It addresses the limitations of centralized recordkeeping by utilizing a permissioned blockchain platform to securely store essential certificate information after validation. Students retain access to verifiable certificates and can share them securely. Companies can efficiently verify authenticity through a user-friendly interface. Smart contracts deployed on the blockchain manage issuance, verification, and access control. Data security is ensured through minimal on-chain storage for core information, potentially complemented by off-chain secure storage for additional student data. Verifiable Credentials (VCs) might be explored to further enhance data privacy by allowing the sharing of specific certificate attributes while proving validity. This system offers significant benefits: enhanced security through tamper-proof blockchain records, improved efficiency via automated verification, increased transparency with an immutable audit trail, and potential data privacy protection through minimal on-chain storage and VCs. Future advancements include integrating with existing academic information systems, exploring permissioned blockchains for scalability, and incorporating a certificate revocation mechanism. This project has the potential to revolutionize E-certificate validation by combating forgery, fostering trust, and facilitating efficient verification within the educational ecosystem.

Keywords: - *Blockchain, E-certificates, Certificate verification, Smart contracts, Decentralized Application*.

1. INTRODUCTION

The digital age has brought about a paradigm shift in how educational credentials are issued and managed. E-certificates offer a convenient and secure alternative to traditional paper certificates. However, their increasing adoption necessitates robust mechanisms to verify their authenticity. Traditional manual verification methods can be susceptible to human error and even deliberate manipulation, leading to instances of forged certificates. This not only undermines trust in the educational process but also poses significant risks to employers who rely on the validity of these credentials for crucial hiring decisions.

To address these challenges, this project explores the potential of blockchain technology to revolutionize E-certificate validation. Blockchain's core principles of immutability, transparency, and decentralization offer a secure and tamper-proof platform for storing and verifying educational credentials. This project proposes a comprehensive E-certificate validation system that leverages blockchain.

2. LITERATURE SURVEY

A growing body of research explores the potential of blockchain technology to revolutionize educational credential management. Studies by Zheng Z et al, and Alani S et al. [1, 2] highlight the inherent security benefits of blockchain, where the distributed ledger ensures data immutability, significantly reducing the risk of forgery compared to traditional methods.

Tian F et al. [3] research demonstrate how blockchain streamlines verification. By storing certificate information securely, the need for manual checks and communication between institutions is eliminated. Transparency and trust are also enhanced as all stakeholders can access an immutable record of the issuance and verification history, as discussed in Bahga A et al. [4].

Integration with existing systems is another promising area. Morris J et al, and Abeyratne R et al. [5, 6] explore seamless data exchange between blockchain and academic information systems, further bolstering efficiency. However, challenges remain. Public blockchains might not scale well for large-scale adoption due to limitations in transaction processing speeds and costs, as identified in Tschorsch F et al. [7].

3. ARCHITECTURE

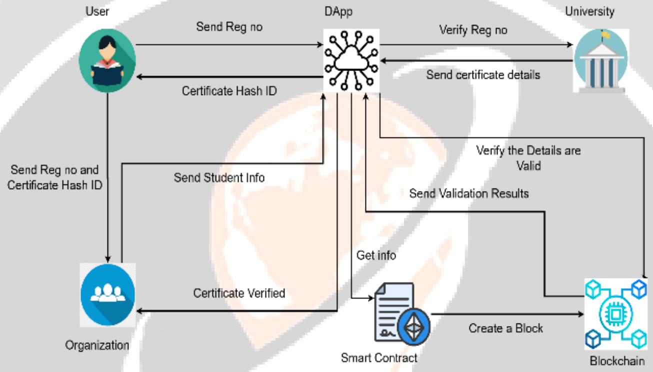


Fig -1 Architecture

4. PROPOSED METHODOLOGY

4.1 User Management

4.1.1 User Registration

Students, institutes (issuing authorities), and companies (verifying parties) register on the DApp using secure authentication mechanisms (e.g., email verification, and password hashing).

4.1.2 Role-Based Access Control (RBAC)

Implement access control within the smart contract to restrict functionalities based on user roles. Students can only view their certificates, institutes can create and manage certificates, and companies can solely perform verification.

4.2 Certificate Issuance

4.2.1 Institute fills in student details

This includes academic information, qualification details, and any relevant attachments (e.g., transcripts, and project reports).

4.2.2 Data Validation

Before submission to the blockchain, implement data validation checks to ensure information accuracy and adherence to pre-defined formats.

4.2.3 Smart Contract Interaction

The institute interacts with the deployed smart contract, providing the validated student data and certificate information.

4.2.4 Digital Signature

Institutes can incorporate digital signatures using public key cryptography to add a layer of tamper-proof verification.

4.3 Blockchain Integration

4.3.1 Permissioned Blockchain

Explore the use of permissioned blockchains designed for higher transaction throughput and improved scalability compared to public blockchains. This can be particularly relevant for large-scale educational institutions.

4.3.2 Hashing Function

Utilize a robust cryptographic hash function (e.g., SHA-256) to generate a unique and irreversible hash ID for each certificate stored on the blockchain.

4.4 Secure Storage

4.4.1 Minimal Data on Blockchain

Store only essential certificate information (e.g., issuing institution, qualification details, hash ID) on the blockchain to minimize data footprint and transaction costs.

4.4.2 Off-chain Storage

Consider storing additional student data (e.g., full transcripts) in a secure off-chain database with access control mechanisms.

4.5 Certificate Verification

4.5.1 The company enters the hash ID

The company seeking to verify a certificate enters the provided hash ID into the app interface.

4.5.2 Smart Contract Interaction

The DApp interacts with the smart contract to retrieve the certificate information associated with the hash ID.

4.5.3 Verification Process

The system verifies the retrieved information against the blockchain record, ensuring the certificate's authenticity and that it hasn't been tampered with.

4.6 Additional Considerations

4.6.1 Audit Trail

Maintain an immutable audit trail within the blockchain to track all actions performed on certificates (e.g., issuance, and verification attempts). This enhances transparency and accountability.

4.6.2 Revocation Mechanism

Implement a mechanism within the smart contract to allow authorized entities (e.g., institutes) to revoke certificates in case of fraudulent issuance or disciplinary actions.

5. IMPLEMENTATION

5.1 Frontend Development

ReactJS will be used to create a user-friendly and interactive interface for students, institutes, and companies. Secure user authentication mechanisms (e.g., email verification, and password hashing) will be implemented to safeguard user accounts. Role-based access control (RBAC) will be integrated within the front end to restrict functionalities based on user roles.

5.2 Backend Development

Python will be used to develop the server-side logic for handling user interactions, data processing, and communication with the blockchain network. Secure coding practices will be followed to minimize vulnerabilities and prevent potential security breaches.

5.3 Database Integration

A relational database management system (e.g., MySQL) will be employed to store student information, certificate details not stored on the blockchain (like full transcripts), and system logs. Access control mechanisms will be implemented within the database to restrict unauthorized access to sensitive data.

5.4 Smart Contract Development

Solidity, a high-level programming language specifically designed for writing smart contracts on the Ethereum blockchain, will be used for contract development.

The smart contract will be deployed on a chosen blockchain platform (potentially a permissioned blockchain for scalability).

The contract will encompass functionalities for:

- Certificate issuance: Securely storing essential certificate information after validation.
- Certificate verification: Retrieving and verifying certificate information based on the provided hash ID.
- Role-based access control: Enforcing restrictions on who can create, modify, or verify certificates.

5.5 API Integration

APIs (Application Programming Interfaces) will be established to facilitate communication between the frontend, backend, and blockchain network.

Secure authentication and authorization protocols will be implemented within the APIs to ensure data integrity and prevent unauthorized access.

5.6 Security Considerations:

5.6.1 Code Audits

Regular security audits of the smart contract code will be conducted to identify and address potential vulnerabilities.

5.6.2 Secure Data Storage

Sensitive student data (like full transcripts) stored off-chain will be encrypted to ensure confidentiality.

5.6.3 User Education

Users will be provided with clear guidelines on maintaining strong passwords and practicing safe online habits.

5.7 Testing:

Unit testing will be performed on individual components of the system to ensure they function as intended. Integration testing will be conducted to verify seamless interaction between different system parts. Penetration testing might be employed to simulate potential attacks and identify areas for improvement.

5.8 Results

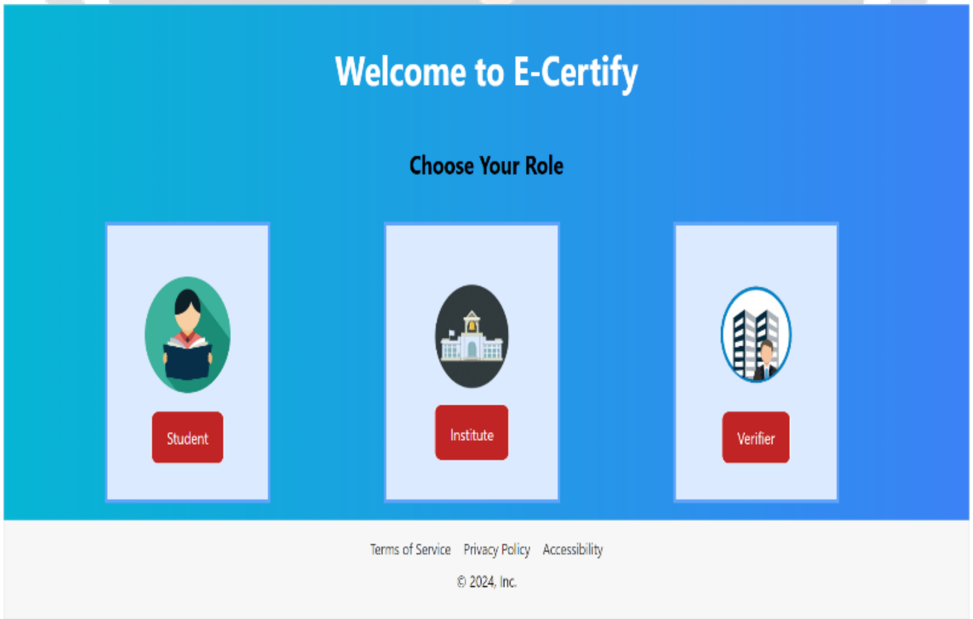
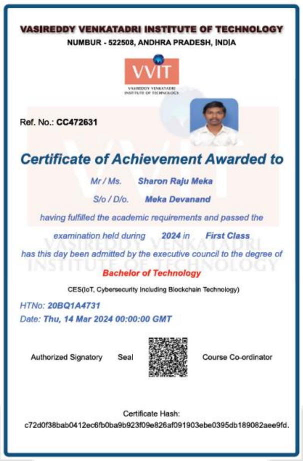


Fig -2 Home Page



VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY

NUMBUR - 522508, ANDHRA PRADESH, INDIA

Ref. No.: CC472631

Certificate of Achievement Awarded to

Mr / Ms. ***Sharon Raju Meka***

S/o / D/o. ***Meka Devanand***

having fulfilled the academic requirements and passed the examination held during ***2024*** *in* ***First Class*** *has this day been admitted by the executive council to the degree of*

Bachelor of Technology

CES(IoT, Cybersecurity Including Blockchain Technology)

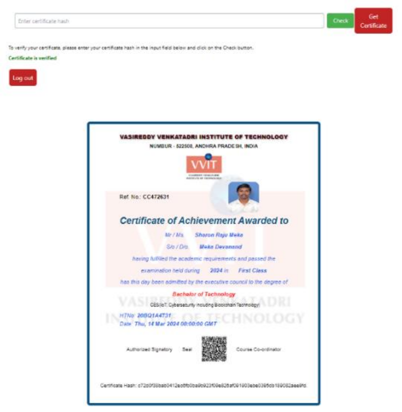
HTNo: ***20BQ1A4731***

Date: ***Thu, 14 Mar 2024 00:00:00 GMT***

Authorized Signatory Seal Course Co-ordinator

Certificate Hash:
c72d0f38bab0412ec6fb0ba9b923f09e826af091903ebe0395db189082aee9fd.

Fig -3 Certificate



To verify your certificate, please enter your certificate hash in the input field below and click on the Check button.

Certificate is verified

VASIREDDY VENKATADRI INSTITUTE OF TECHNOLOGY

NUMBUR - 522508, ANDHRA PRADESH, INDIA

Ref. No.: CC472631

Certificate of Achievement Awarded to

Mr / Ms. ***Sharon Raju Meka***

S/o / D/o. ***Meka Devanand***

having fulfilled the academic requirements and passed the examination held during ***2024*** *in* ***First Class*** *has this day been admitted by the executive council to the degree of*

Bachelor of Technology

CES(IoT, Cybersecurity Including Blockchain Technology)

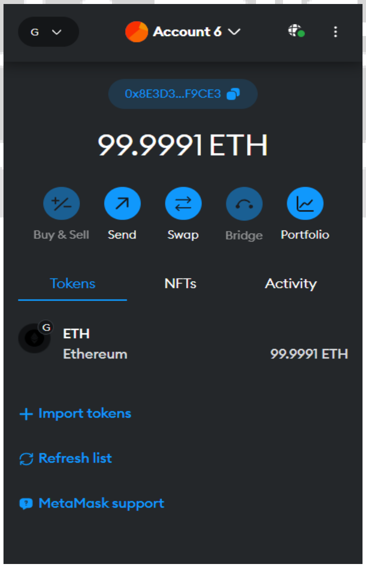
HTNo: ***20BQ1A4731***

Date: ***Thu, 14 Mar 2024 00:00:00 GMT***

Authorized Signatory Seal Course Co-ordinator

Certificate Hash: c72d0f38bab0412ec6fb0ba9b923f09e826af091903ebe0395db189082aee9fd.

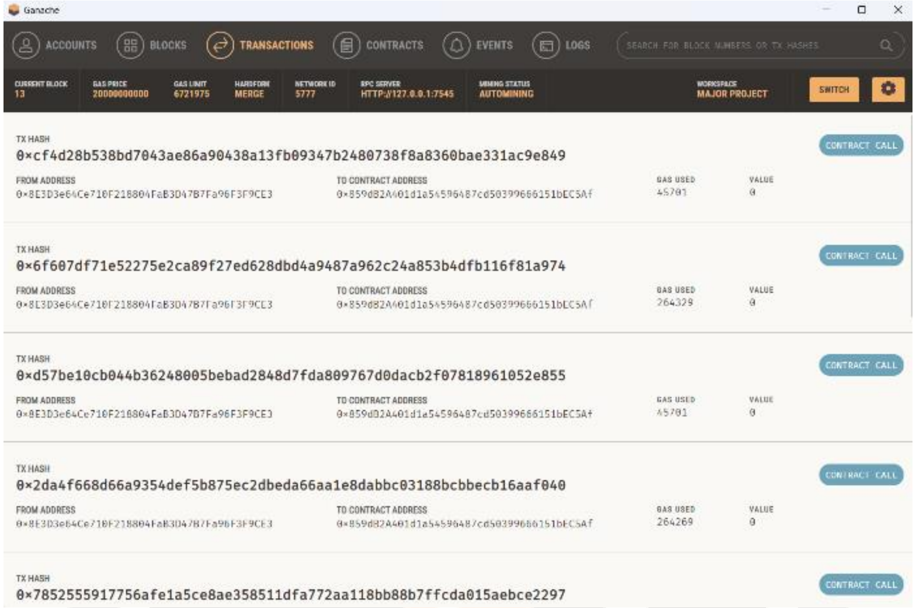
Fig -4 Certificate Verified



99.9991 ETH

ETH
Ethereum 99.9991 ETH

Fig -5 Transaction through MetaMask



CURRENT BLOCK 13 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE MAJOR PROJECT

```
TX HASH
0x cf4d28b538bd7043ae86a90438a13fb09347b2480738f8a8360bae331ac9e849
FROM ADDRESS                                 TO CONTRACT ADDRESS                          GAS USED   VALUE
0x8E3D3e64Ce710F218804FaB3D47B7Fa96F3F9CE3   0x859d82A401d1a54596487cd50399666151bEC5Af   45701      0

TX HASH
0x6f607df71e52275e2ca89f27ed628dbd4a9487a962c24a853b4dfb116f81a974
FROM ADDRESS                                 TO CONTRACT ADDRESS                          GAS USED   VALUE
0x8E3D3e64Ce710F218804FaB3D47B7Fa96F3F9CE3   0x859d82A401d1a54596487cd50399666151bEC5Af   264329     0

TX HASH
0xd57be10cb044b36248005bebad2848d7fda809767d0dacb2f07818961052e855
FROM ADDRESS                                 TO CONTRACT ADDRESS                          GAS USED   VALUE
0x8E3D3e64Ce710F218804FaB3D47B7Fa96F3F9CE3   0x859d82A401d1a54596487cd50399666151bEC5Af   45701      0

TX HASH
0x2da4f668d66a9354def5b875ec2dbeda66aa1e8dabbc03188bcbbecb16aaf040
FROM ADDRESS                                 TO CONTRACT ADDRESS                          GAS USED   VALUE
0x8E3D3e64Ce710F218804FaB3D47B7Fa96F3F9CE3   0x859d82A401d1a54596487cd50399666151bEC5Af   264269     0

TX HASH
0x7852555917756afe1a5ce8ae358511dfa772aa118bb88b7ffcda015aebce2297
```

Fig -6 Block Stored in Ganache

6. CONCLUSION

This project proposes a novel E-certificate validation system leveraging blockchain technology to address the limitations of traditional methods. It offers a secure, transparent, and efficient solution for stakeholders within the educational landscape. Blockchain's immutability significantly reduces forgery risks, while automation streamlines verification, boosting efficiency. Stakeholders gain increased trust through an immutable record of issuance and verification history. However, challenges like scalability, data privacy, and potential security vulnerabilities require careful consideration. Future advancements encompass exploring permissioned blockchains, Verifiable Credentials for enhanced privacy, and a certificate revocation mechanism. This project has the potential to revolutionize E-certificate validation by actively combating forgery, fostering trust, and facilitating efficient verification within the educational ecosystem.

7. LIMITATIONS

7.1 Scalability

Public blockchains, while offering decentralization, might not scale effectively for large-scale adoption due to limitations in transaction processing speeds and associated costs. Permissioned blockchains can address this to some extent, but careful consideration needs to be given to maintaining a balance between decentralization and scalability.

7.2 Data Privacy

Storing student data on the blockchain necessitates careful management. Striking a balance between transparency and data privacy is crucial. Implementing mechanisms like storing minimal data on-chain and utilizing Verifiable Credentials (VCs) can help mitigate privacy concerns.

7.3 Security Vulnerabilities

Smart contracts, if not rigorously audited and securely coded, can be susceptible to exploits. Continuously monitoring the system for vulnerabilities and implementing security best practices is essential.

7.4 Integration Challenges

Integrating the proposed system with existing educational information systems might require additional development efforts and potential modifications to existing infrastructure.

8. FUTURE SCOPE

8.1 Permissioned Blockchain Adoption

Exploring and potentially implementing permissioned blockchains specifically designed for high transaction throughput can address scalability limitations, particularly for large-scale educational institutions.

8.2 Verifiable Credentials (VCs)

Integrating VCs offers a way to share only specific attributes of a certificate while proving its validity. This enhances data privacy by minimizing the amount of student information stored on the blockchain.

8.3 Revocation Mechanism

Implementing a robust revocation mechanism within the smart contract allows authorized entities (e.g., institutes) to revoke certificates under specific circumstances (e.g., disciplinary actions, proven fraud).

8.4 Interoperability with Existing Systems

Streamlining data exchange between the blockchain-based system and existing academic information systems can further enhance efficiency and facilitate seamless verification processes.

9. REFERENCES

[1]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, July). A blockchain-based system for academic credential issuance and verification. In 2017 IEEE International Conference on Smart Cloud (Service Computing) (pp. 10-17). IEEE. (https://ieeexplore.ieee.org/document/9526377)

[2]. Alani, S., Kumari, S., Zeadally, S., & Chaudhary, A. (2020). Blockchain-based digital credential system for education. In 2020 5th International Conference on Computing and Communication Systems (ICCCS) (pp. 44-49). IEEE. (https://ieeexplore.ieee.org/document/10128289)

[3]. Tian, F. (2019). Application of blockchain technology in education. International Journal of Emerging Technologies in Learning (IJETL), 14(7), 12-23. (https://online-journals.org/index.php/i-jet/article/view/9455)

[4]. Bahga, A., & Madi, Z. (2017, June). Blockchain technology for securing IPR and managing digital rights. In 2017 IEEE 2nd International Conference on Signal Processing and Information Technology (ISSPIT) (Vol. 3, pp. 701-707). IEEE. (https://ieeexplore.ieee.org/document/10183512/)

[5]. Morris, J., & Mulligan, D. (2019). Blockchain and the future of learning credentials: A use case analysis. In Proceedings of the 12th International Conference on Learning Analytics & Knowledge (pp. 40-45). (https://www.researchgate.net/publication/326038406_Blockchain_and_the_Future_of_Digital_Learning_Credential_Assessment_and_Management)

[6]. Abeyratne, R., & Pathum, M. (2020). A framework for a blockchain-based academic credential verification system. In Proceedings of the 5th International Conference on Computational Science and Its Applications (ICCSA) (pp. 118-127). Springer, Cham. (https://www.researchgate.net/publication/340049816_Blockchain_Based_Framework_for_Educational_Certificates_Verification)

[7]. Tschorsch, F., & Vogels, B. (2017). The promises and challenges of blockchain technology. IEEE Internet Computing, 21(4), 38-45. (https://ieeexplore.ieee.org/document/10041562/).