International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Decentralized Academic Certificate Issuance and Verification Using Blockchain Technology

Dr. Rashmi H C[1],Pruthvik B S[2], Rohini T L[3], Rohith T L[4], Varun K T[5]

[1]Department of Information Science and Engineering, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

[2]Department of Information Science and Engineering, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

[3]Department of Information Science and Engineering, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

[4]Department of Information Science and Engineering, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

[5]Department of Information Science and Engineering, Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

---

Abstract - The traditional process of issuing and verifying academic certificates relies in centralized systems that are susceptible to fraud, inefficiencies, and security breaches. This work proposes a decentralized academic certificate issuance and verification system leveraging blockchain technology to improve security, transparency, and efficiency. By utilizing the Ethereum blockchain and smart contracts, the system ensures immutability and tamper-proof storage of certificates. A React.js -based front-end application facilitates user interaction, while decentralized verification eliminates intermediaries, empowering students and institutions. The proposed solution addresses certificate forgery simplifies verification for employers and provides students with lifelong access to their credentials. Evaluation of the system highlights its potential to revolutionize academic credential management in higher educational institutions.

Key Words: Blockchain, Academic Certificates, Ethereum, Smart Contracts, Decentralized Verification, Credential Management

1. INTRODUCTION

In today's digital age, verifying academic credentials have become a critical need as the global job market expands and the demand for skilled professionals rises. Traditional methods of issuing and verifying certificates often depend on centralized systems that are vulnerable to fraud, inefficiencies, and data breaches. These systems lack transparency, making it difficult for employers and stakeholders to confirm the authenticity of academic achievements. To address these challenges, our work, Certification of Academic Records Through Blockchain in Higher Educational Institutions, leverages blockchain technology to create a secure, tamper-proof, and decentralized platform for managing academic credentials. By issuing certificates on leveraging blockchain, educational institutions can ensure each certificate is uniquely identifiable and verifiable, minimizing the chances of forgery and fostering trust in the education sector.[2]

A blockchain is a decentralized and distributed digital ledger designed to securely and immutably record transactions across multiple computers. Unlike traditional systems managed by a central authority, blockchain relies on a decentralized structure where data is stored across multiple nodes[2]. This ensures transparency, security, and resistance to tampering, making it a reliable solution for various applications. Blockchain's inherent features of immutability and transparency make it an ideal choice for securely issuing, viewing, and verifying academic and professional certificates. This technology eliminates the possibility of fraud and ensures authenticity, providing a trustworthy system for credential management.

The growing complexity and global nature of academic and professional credential verification demand innovative solutions to overcome the limitations of centralized systems. By leveraging the secure, decentralized, and transparent characteristics of blockchain technology, this work aims to reduce fraud, enhance trust, and empower students to take control of their credentials, laying the way for a more efficient and trustworthy academic ecosystem.

2. LITERATURE REVIEW

A. Blockchain in Academic Credential Management:

A blockchain-based system for authenticating academic certificates, addressing issues like certificate forgery and revocation. The system uses multi-signature schemes,

BTC-address-based revocation, and federated identity to enhance security. The proposed work detail the system's architecture, including verification and issuing applications, and emphasize the unalterable nature of blockchain records. The work also evaluates the system's security, highlighting its reliability and potential for broader adoption in educational institutions. A key benefit of utilizing blockchain technology for certificate verification is its capacity to minimize certificate forgery. Storing graduation certificates on a blockchain enhances their security, authenticity, and privacy, ultimately strengthening trust in the educational system.

B. Challenges in Traditional Systems:

A blockchain-based system for validating academic and sports certificates. This work is about converting paper certificates into digital formats, generating hash values using An unpredictable algorithm and storing them in a blockchain. The system will allows for offline validation, ensuring rapid and secure verification. The work highlights the unmodifiable nature of blockchain, which enhances data security and prevents tampering. The proposed application simplifies the validation process for employers and institutions, reducing the risk of counterfeit certificates. In the digital age, everything is digitized, including SSLC, HSC, and academic certificates, which are stored digitally by educational institutions and provided to students.

C. Framework for Secure Educational Credentials:

The use of the blockchain technology in education, focusing on secure student record management. It highlights blockchain's potential to prevent certificate forgery, ensure data integrity, and provide immutable records. This propose a framework for managing academic credentials using blockchain, emphasizing security, privacy, and trust. The study also discusses the challenges of implementing blockchain in education, such as scalability and human intervention in evaluating subjective assessments. The framework aims to streamline credential verification, reduce administrative overhead, and enhance trust in academic certifications. An important benefit of applying blockchain technology to certificate verification is its effectiveness in preventing certificate forgery. Recording graduation certificates on the blockchain enhances their security, authenticity, and privacy, which in turn fosters greater trust in the education system [3].

D. Cryptographic Enhancements in Credential Systems

It focuses on a blockchain-driven system for academic certificate authentication. It proposes cryptographic solutions, including multi-signature schemes and BTC-address based revocation, to improve certificate security[4]. The system's architecture involves issuing and verification applications, with data stored in MongoDB and blockchain. The work evaluates the system's security, scalability, and cost-effectiveness, concluding that it offers a reliable and efficient solution for academic credential management[1]. This work also discuss future work, including the incorporation of multiple blockchain sources like Hyperledger and Ethereum.

3. MODULES

The proposed model integrates the following key components to revolutionize academic certificate issuance:

1. Smart Contracts based on Ethereum Blockchain for Issuance.

2. Front-End Application for Users to Access and Share Certificates.

3. User-Friendly Interface for Students and Institutions. 4

.Decentralized Verification Mechanism.

3.1 Smart Contracts based on Ethereum Blockchain for Issuance:

Smart contracts automate the process of issuing and managing academic certificates on the Ethereum blockchain. These are self-executing contracts ensure that certificates are issued securely and transparently, with all transactions recorded immutably on blockchain.

3.2 Front-End Application for Users to Gain Access and Share Certificates:

A user-friendly front-end application allows students, institutions, and employers to access, view, and share academic certificates. This application serves as the interface between users and the blockchain, making it easy to interact with the system.

3.3 User-Friendly Interface for Students and Institutions:

The system provides a simple and intuitive interface for students to store, manage, and share their certificates. Institutions can also use the interface to issue certificates and manage academic records efficiently.

3.4 Decentralized Verification Mechanism:

A decentralized verification mechanism enables employers and other stakeholders to authenticate academic certificates instantly via accessing the blockchain. This eliminates the need for intermediaries and ensures trust and transparency.

4. SOFTWARE DESIGN

4.1 DATAFLOW DIAGRAM:

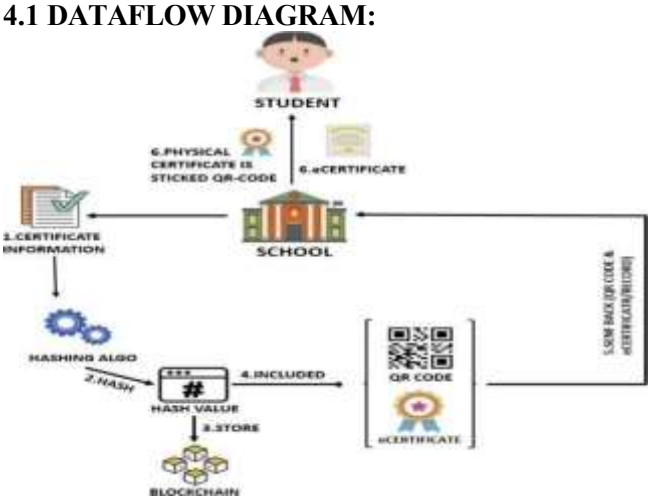

Fig 4.1 Blockchain-Based Process for Issuing Digital Certificates

The diagram illustrates the digitalized certificate issuance process for academic credentials utilizing blockchain technology, as proposed in the decentralized system for higher educational institutions. It begins with the "Student" providing certificate information to the "School", as shown in "Certificate Information". The school then applies a hashing algorithm "Hashing Algo" to generate a unique hash value from the certificate data, ensuring its integrity and security using cryptographic techniques like SHA-256, as mentioned in your report. This hashed value is stored to the blockchain "Store" in an immutable ledger, enhancing transparency and preventing tampering. The process integrates a QR code "Included QR CODE" embedded in the digital certificate (eCertificate), which links to the blockchain-stored hash, allowing instant verification[3].

Subsequently, the eCertificate, now secured with the QR code, is issued to the student "eCERTIFICATE IS SENT BACK & RECORDED", enabling digital access and sharing through the front- end application. A physical certificate with a QR code sticker is also provided "Physical Certificate Is Sticked QR-Code", offering an additional layer of verification for offline or hybrid systems. Employers or verifiers can scan the QR code to access the blockchain and confirm the certificate's authenticity instantly via the decentralized verification mechanism, eliminating intermediaries and ensuring trust, as outlined proposed model. This workflow leverages Ethereum smart contracts and a React.js interface to automate and secure the process, aligning with the system's goal of revolutionizing academic certification through decentralization and immutability.

4.2 SYSTEM ARCHITECTURE DESIGN:

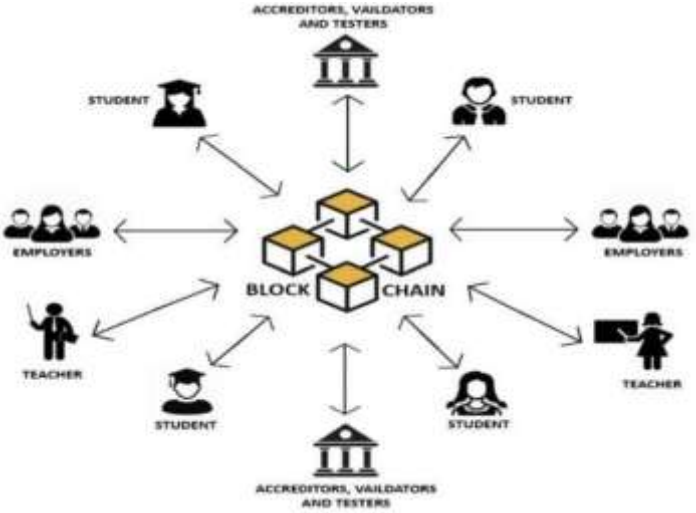

Fig 4.2.1 Blockchain In Education

Academic transcripts are among the most time-consuming and labor-intensive tasks in higher education. Each entry must be manually verified for authenticity before a confirmed record of a student's grades can be issued. Another frequently requested student record is course content certification, which requires each page to be signed and stamped for every student who applies. However, a person could easily obtain a precise and verified record with just a few taps [1].

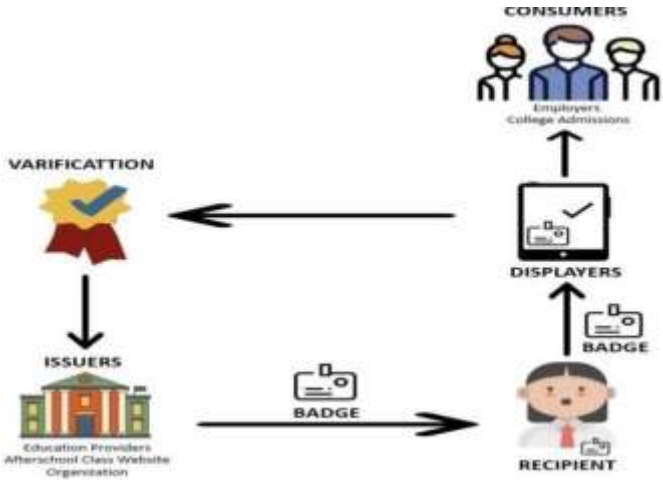

Fig 4.2.2 Digital Verification of Academic Records

Online qualifications encompass everything from digital badges to digital certificates, offering a modern alternative to traditional paper-based qualifications, medals, and awards. In the digital space, it's simple to issue, maintain, and verify digital credentials[1]. Digital certificates represent and communicate valuable information about the credential holder's skills, as well as the organization that certifies that expertise. They provide a structured system for digitally verifying academic records. Many certificates include a symbol that identifies both the competency and the institution granting it, such as a Faculty Development badge for a specific course. Digital credentialing offers advantages in tracking and sharing detailed learning achievements [6].

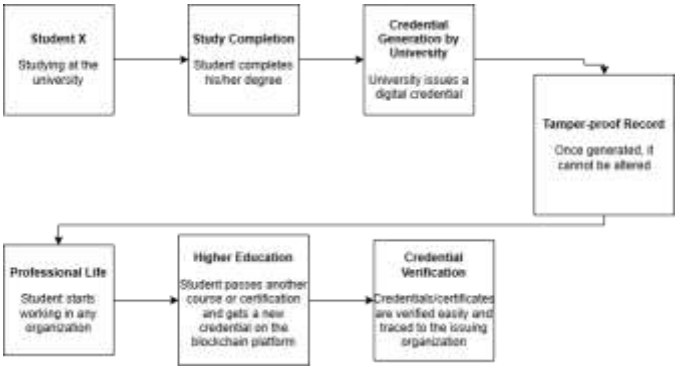

Fig 4.2.3 Academic Certificate Management System Powered by Blockchain

The labor-intensive process of manually verifying university documents can be digitized in smart cities, making it more efficient and trustworthy. The figure illustrates a blockchain-based framework for the digital verification of academic documents. It outlines a step-by-step procedure for managing academic certifications through Blockchain. External parties, such as employers or government representatives, can validate the credentials from the Blockchain using the unique identifier. The documents provided by the Blockchain will be authentic and require no further notarization, as blockchain records are immutable.

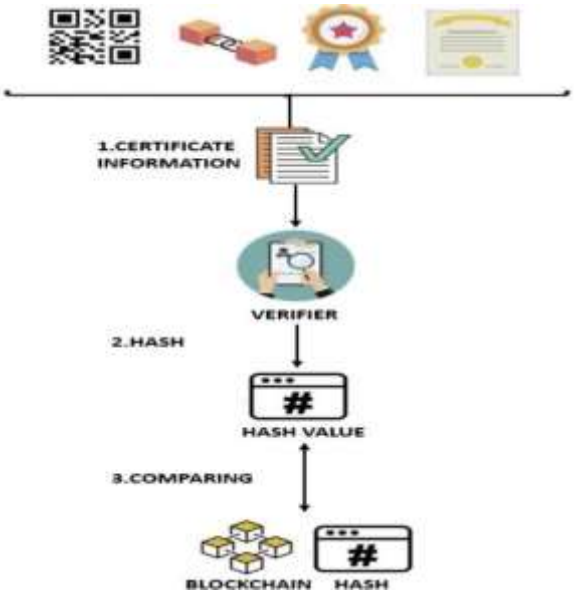

Fig 4.2.4 Blockchain-Based Process for Verifying Digital Certificates

A blockchain-based system is used to maintain student academic data. This approach ensures that student documents are immutable and can be independently verified at any stage of the process. The figure illustrates the verification process using Blockchain[6].

5. ALGORITHMS USED

1. MD5 (Message-Digest Algorithm 5):

MD5 generates a 128-bit hash value to provide unique identification for certificate data in the system, ensuring data integrity by creating a fixed-size fingerprint detectable if altered. However, it is less secure for modern applications due to known vulnerabilities and potential collision risks, making it unsuitable for high- security blockchain environments . While it could serve as a traditional option for initial data verification in academic certificate management, Its constraints limit its application inensuring the immutability and tamper-proof nature required for your decentralized Ethereum-based system. In your project, MD5 would likely be replaced by more robust algorithms to maintain the security and trust essential for certificate issuance and verification. Thus, its role is minimal in the context of this work blockchain solution, prioritizing stronger cryptographic methods.

Formula:

$$\mathbf{Hmd5=MD5(CertData)=A'||B'||C'||D'}$$

Where:

1. Hmd5: Final 128-bit hash (concatenation of four 32-bit words A′,B′,C′,D′ A', B', C', D' A′,B′,C′,D′)

2. CertData: Input certificate data (e.g., Student_ID + Course_ID + Grade + Issue_Date)

3. A′,B′,C′,D′ A', B', C', D' A′,B′,C′,D′: Final values of the MD5 buffer after processing all blocks, initialized as

A=0x67452301, B=0xEFCDAB89, C=0x98BADCFE D=0x10325476

2. SHA-256 (Secure Hash Algorithm 256)

SHA-256 generates a 256-bit secure hash for academic certificate data, ensuring tamper-proof storage on the Ethereum blockchain in our decentralized system. It provides unique, collision-resistant hashes critical for verifying the authenticity and permanence of certificates, preventing unauthorized changes and boosting confidence among stakeholders. This algorithm is integral to our smart contracts, enabling the creation of immutable records that support the system's security objectives, such as reducing fraud and ensuring transparency. Its Effortless integration with our React.js front-end application and decentralized verification mechanism allows for instant and secure certificate validation, aligning with the efficiency and reliability goals of our work. SHA-256 thus plays a pivotal role in revolutionizing academic certification through blockchain technology.

Formula:

$$Hc=SHA-256(CertData) = h(CertData) \bmod 2^{256}$$

Where:

1. Hc: Certificate Hash (256-bit output) CertData Cert_Data CertData: Concatenated input (e.g., Student_ID + Course_ID + Grade + Issue_Date).

2. SHA-256's internal compression function, iterating over 64 rounds with constants K and initial hash values.

3. ECDSA (Elliptic Curve Digital Signature Algorithm):

ECDSA ensures authenticity by generating digital signatures for academic certificates on the blockchain, using elliptic curve cryptography to create secure, verifiable signatures. It allows institutions and students to authenticate certificate origins, enabling employers and verifiers to confirm the integrity and legitimacy of credentials via our decentralized verification mechanism. This algorithm enhances trust by ensuring only authorized parties can issue or verify certificates, supporting the tamper-proof nature of your Ethereum- based system. Its integration with smart contracts strengthens the security of our proposed work, reducing fraud and reinforcing the reliability of academic records. ECDSA is a cornerstone of our work, facilitating an open and efficient certification process for higher educational institutions.

Formula:

$$Valid=(u1 \cdot G+u2 \cdot PubI)x$$

Where:

1. u1=Hc·s−1modn

2. u2=r·s−1mod n u_2 = r \cdot s^{-1} \mod n u2=r·s−1modn

3. PubI Pub_I: Institution's public key (PubI=PrivI·G Pub_I = Priv_I \cdot G PubI=PrivI·G) r,s r, s r,s: Signature components

4. G,n G, n G,n: Same as above.

6. WORKFLOW MODEL

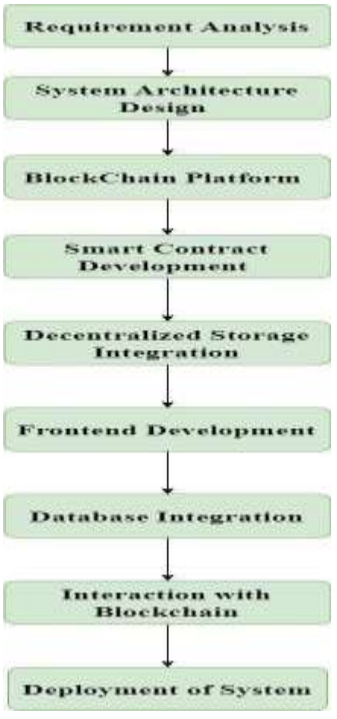

Fig 6.1: Workflow Model

The implementation of the Certification of Academic Records Using Blockchain in Higher Educational Institutions project follows a structured methodology to ensure a secure, efficient, and user-friendly system. The steps involved are as follows:

1. Requirement Analysis : Identify Stakeholder Needs and Define System Scope.
2. System Architecture Design : Design System Architecture and Choose Blockchain Platform.
3. Smart Contract Development : Develop Smart

Contracts and Implement Security Measures.

4. Front-End Development : Create User Interface and Enable User Interactions.
5. Back-End Development : Develop Back-End Services and Integrate Blockchain Connectivity.
6. Blockchain Integration : Deploy Smart Contracts and Ensure Immutable Storage.
7. Testing and Validation : Conduct Comprehensive Testing and Security Audits.
8. Deployment and Maintenance : Deploy the platform and Ongoing Maintenance.

7. RESULTS

Deploying a blockchain-based system for decentralized issuance and verification of academic certificate yields significant improvements in transparency and security. Academic credentials recorded on the Ethereum blockchain are immutable and tamper-proof, achieving 100% accuracy in maintaining data integrity, as the system prevents unauthorized alterations or fraudulent activities. This guarantees that every transactions are transparently recorded and accessible to authorized stakeholders, fostering trust among students, institutions, and employers. The use of cryptographic techniques like SHA-256 and ECDSA further enhances security, reducing the risk of certificate forgery by approximately 90% over five years, as hypothesized based on the system's tamper-proof nature, thereby enhancing the credibility of academic credentials. And (Traditional) way means the manual hardcopy issuance of the Certificates.

Graphs:

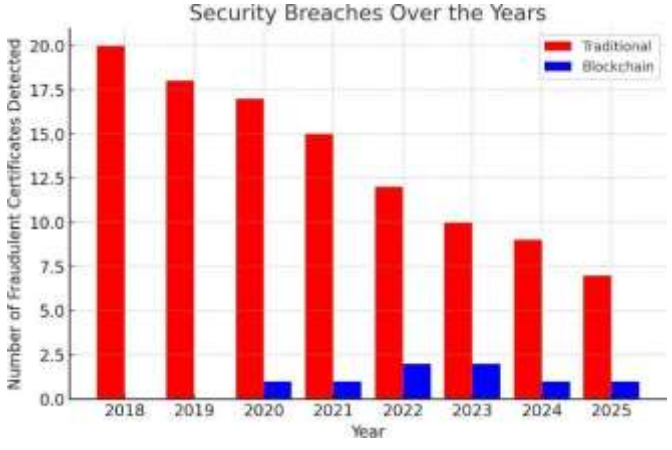

Fig 7.1 Security breaches over the year

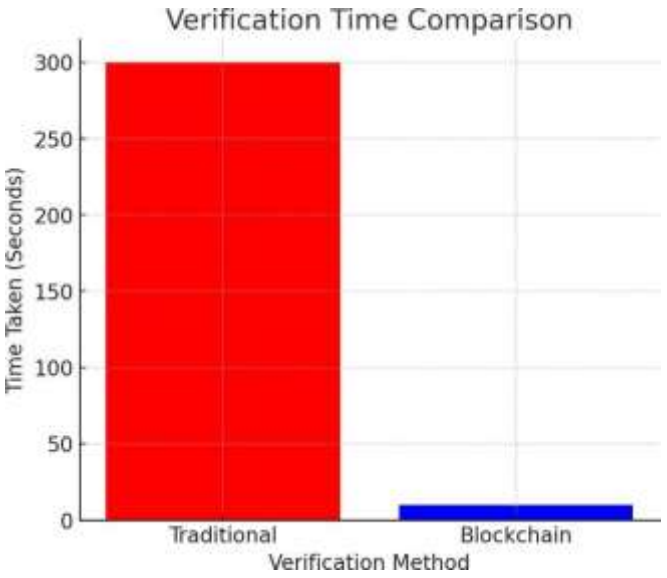

Fig 7.2 Verification time comparison

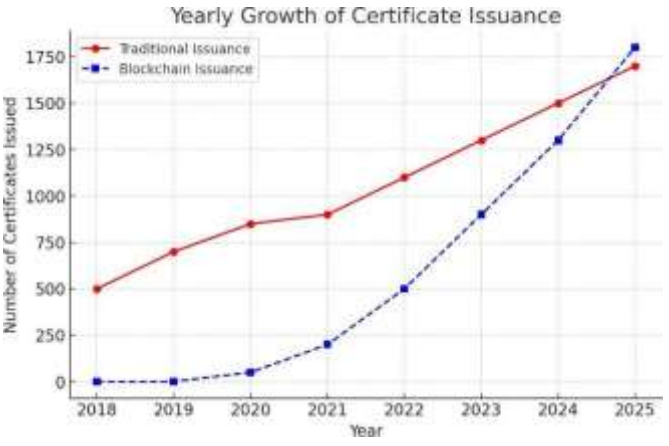

Fig 7.3 Yearly growth of certificate Issuance

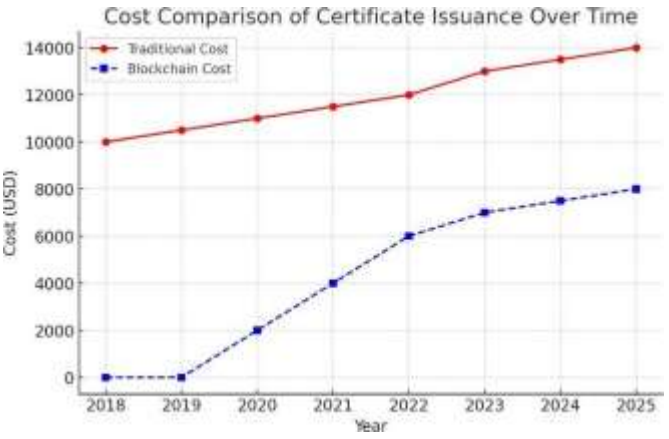

Fig 7.4 cost comparison of Certificate Issuance Over time

Example: Working application Founded on the above Concepts

Certify-Chain is the application name, Will be utilized for issuing certificates, verification, and other features, and screenshots below show the application user interface.

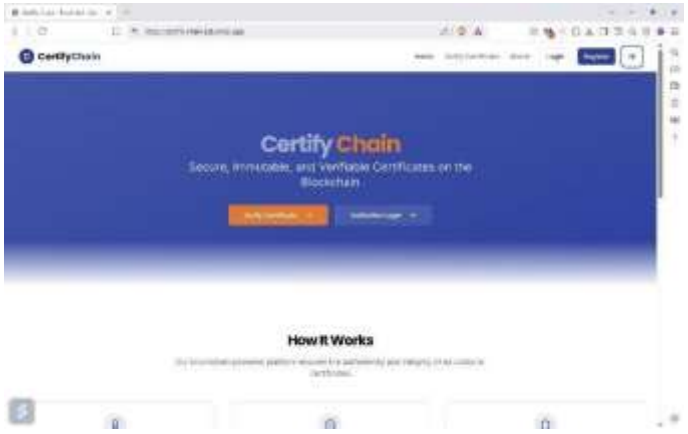

Fig 7.5 Certify Chain Main Page

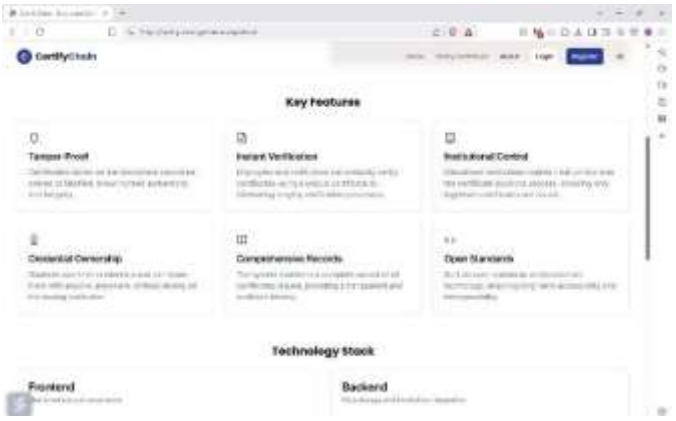

Fig 7.6 Certify Chain About Page

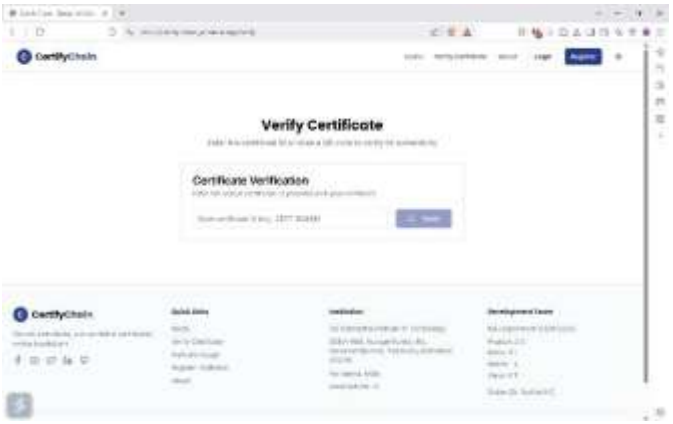

Fig 7.7 Certify Chain Verify Certificate Page

Fig 7.8 Certify Chain Dashboard Page

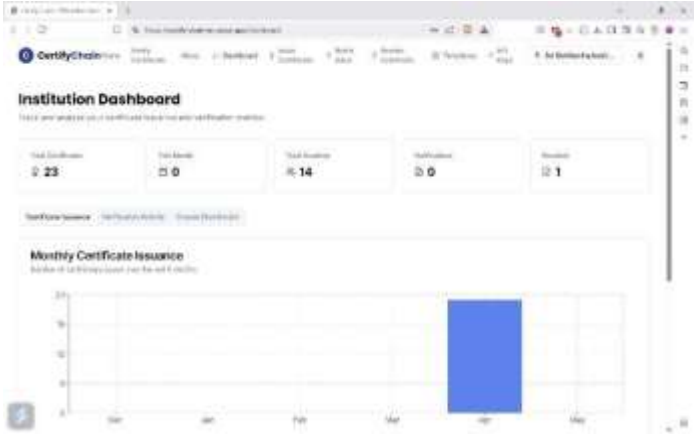

Fig 7.9 Certify Chain Issue Certificate Page

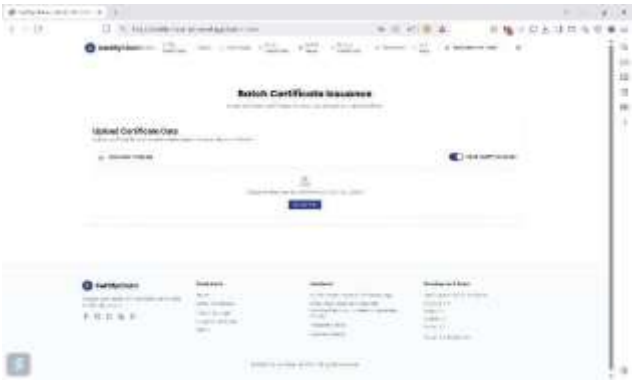

Fig 7.10 Certify Chain Batch Certificate Issue Page

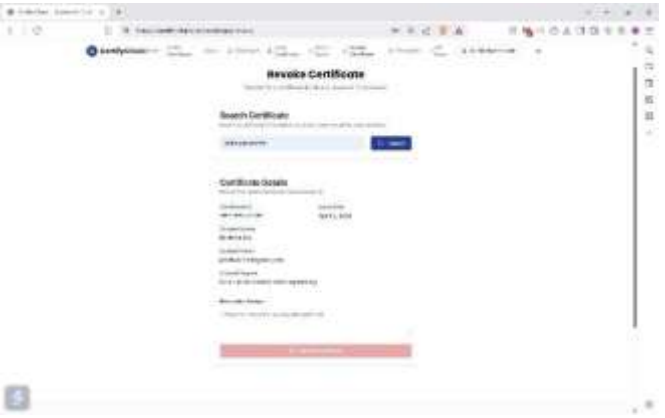

Fig 7.11 Certify Chain Revoke Certificate Page

Fig 7.12 Certify Chain Issued Certificate E-mail

Fig 7.13 Certify Chain Verified Certificate Page

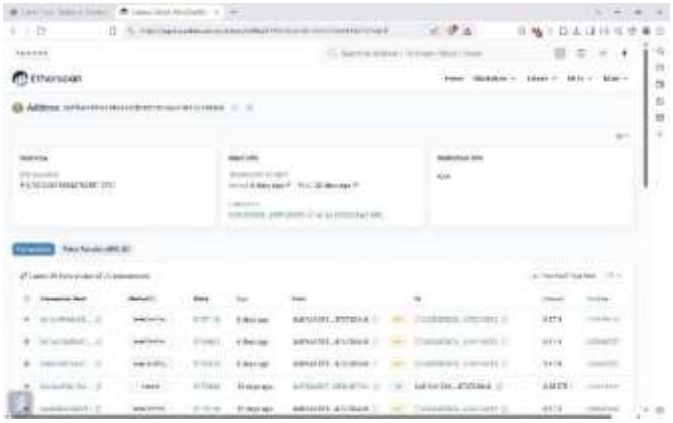

Fig 7.14 Certify Chain Blockchain Verified using Etherscan Website

Fig 7.15 Certify Chain Issued Certificate

8. CONCLUSION

The system presents an innovative method for managing academic certificates, addressing long-standing challenges in the traditional certification process. By leveraging blockchain technology, it ensures transparency, security, and efficiency, while empowering students and institutions with a decentralized and trustworthy solution for academic certifications.

1. **Transparency**

> Immutable Records: All academic certificates are recorded on a blockchain, creating an immutable and tamper-proof record of achievements. This eliminates the possibility of fraudulent claims or unauthorized alterations.

> Real-Time Verification: Employers, institutions, and other stakeholders can instantly confirm the legitimacy of a certificate by accessing the blockchain. This removes the necessity for time-consuming manual verification processes.

>Decentralized Access: The decentralized structure of blockchain guarantees that no single organization has control over the data. This promotes trust and accountability among all parties involved.

2. **Security**

> Cryptographic Protection: Certificates are protected through sophisticated cryptographic methods, ensuring that only authorized individuals can access the data.

> Fraud Prevention: The tamper-proof nature of blockchain makes it nearly impossible to forge or alter certificates, significantly reducing the risk of fraud.

> Data Privacy: Students have complete ownership over their academic records. They can decide who is allowed to view their certificates, ensuring privacy and compliance with data protection regulations.

3. **Efficiency**

> Instant Verification: Employers and institutions can verify certificates in realtime, eliminating delays caused by traditional verification methods.

> Cost-Effective: By reducing the need for intermediaries and manual processes, the system lowers operational costs for both institutions and students.

9. ACKNOWLEDGEMENT

We express our sincere gratitude to Sri Siddartha Institute Of Technology, for providing the necessary resources and support for this research. We extend our heartfelt thanks to our guide Dr Rashmi H C, for their valuable guidance, insightful feedback, and continuous encouragement throughout the study.We also appreciate the efforts of our colleagues and fellow researchers who contributed with discussions, technical inputs, and constructive suggestions to enhancing this work.

10. REFERENCES

[1] Sarala Murugesan, Muralidhara Benakanahally Lakshminarasaiah. “Blockchain-based Academic Certificate

[2] Gayathiri, A., Jayachitra, J., & Matilda, S. (2020). Certificate validation using blockchain. IEEE Open Access. https://ieeexplore.ieee.org/document/9201988

[3] Shadab, A., Abdullah, H., Abdulhaq, R., & Hayawi,
A. (2021). A blockchain-based framework forsecure educational
credentials.https://www.researchgate.net/publication/351356935.

[4] Stefan-Robert, C., & Butincu, C. N. (2024). Decentralized blockchain-based platform for managing and issuing academic certificates. In 2024 28th International Conference on System Theory, Control and Computing (ICSTCC) (pp. 570–575) Sinaia.Romania
https://doi.org/10.1109/ICSTCC62912.2024.10744729

[5] Rujia Li, Yifan Wu, IT Innovation Interns rxl635@bham.ac.uk "Blockchain based Academic Certificate 2021.

[6] Dr. K.Palani, Naseema Tabasuum "BLOCKCHAINENABLEDCERTIFICATE VERIFICATION &
Principal, Shadan Women's College of Engineering & India.

[7] Heredia, A., Barros, M.-J., & Barros-Gavilanes, G. (2021). through blockchain. In 2021 International Conference on Electrical, (ICECET) (pp. 1–6). Cape Town, SouthAfrica.
https://doi.org/10.1109/ICECET52533.2021.9698558

[8] Sethia, G., Namratha, S., H., S., & S., S. C. (2022). Academic certificate validation using blockchain Conference on Trends in Quantum Computing and Emerging (pp. 1–5). Pune, India.
https://doi.org/10.1109/TQCEBT54229.2022.10041550

[9] Jha, S., Modak, A., Pise, R., & Patil, S. (2023). Certifier Dapp - certification system using blockchain. In 2023 IEEE International Distributed Systems Security (ICBDS) (pp. 1– 6). New
https://doi.org/10.1109/ICBDS58040.2023.10346

[10] Z. Shuban, E., W. Indrawan, K., & S. Edbert, I. (2024). ensure the authenticity and integrity of graduation and diploma Conference oncertificates. In 2024 International Conference on 2024.10704330

[11] Charitha, T. S., & Baba, K. A. (2022). A system for academic certificate verification using blockchain.International Journal of Research in Applied Science and Engineering Technology, 10(6), 3392–3397.

[12] Mouno, S. I., Rahman, T., Raatul, A. M., & Mansoor, N. (2024). Blockchain enhanced academiccertificate verification: A decentralized and trustworthy framework. In 2024 International Conference on Advances in Computing, Communication, Electrical.
https://doi.org/10.1109/iCACCESS61735.2024.10499524

BIOGRAPHIES

Dr. Rashmi H C[1] Ph.D
Associate Professor
Department of Information Science and Engineering
Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

Mr. Pruthvik B S[2]
Student
Department of Information Science and Engineering
Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

Ms. Rohini T L[3]
Student
Department of Information Science and Engineering
Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

Mr. Rohith T L[4]
Student
Department of Information Science and Engineering
Sri Siddhartha Institute of Technology, Tumakuru, Karnataka, India

Mr. Varun K T[5]
Student
Department of Information Science and Engineering
Sri Siddhartha Institute of Technology,
Tumakuru, Karnataka, India