VISVESVARAYA TECHNOLOGICAL UNIVERSITY

Jnana Sangama, Belagavi

A

Project Report on

"Blockchain Based Certificate Verification System"

In partial fulfillment of the requirements for the award of the Degree of

BACHELOR OF ENGINEERING

In

Computer Science and Engineering

By

Vishal Prasad Sharma (1AH21CS123)
Anayat Altaf Shah(1AH21CS127)
Raj Kumar(1AH21CS081)
Vandan Kumar M(1AH21CS117)

Under the guidance
of
Mr. Panchaxari Mamadapur
Assistant Professor, Dept. of CSE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

ACS COLLEGE OF ENGINEERING

KAMBIPURA, MYSORE ROAD, BANGLORE-74

2024-2025

ACS COLLEGE OF ENGINEERING

KAMBIPURA, MYSORE ROAD, BANGLORE-74

Department of Computer Science and Engineering

Certificate

Certified that the Project Work entitled **"Blockchain Based Certificate Verification System"** is a bonafide work carried out by **Mr. Vishal Prasad Sharma(1AH21CS123), Mr. Anayat Altaf Shah (1AH21CS127), Mr. Raj Kumar (1AH21CS081) and Mr. Vandan Kumar M (1AH21CS117)** in partial fulfillment for the award of Bachelor of Engineering in Computer science & Engineering of the Visvesvaraya Technological University, Belgaum during the year 2024-2025. It is certified that all the corrections/suggestions indicated for internal assessment have been incorporated in the report deposited in the departmental library. The Project Report has been approved as it satisfies the academic requirements in respect of Project Work prescribed for the said degree.

Signature of Guide	Signature of HOD	Signature of Principal
Mr. Panchaxari Mamadapur	**Dr. T. Senthil Kumaran**	**Dr. Anandthirtha.B. Gudi**
Asst Professor, CSE	Professor & HOD, CSE	Principal
ACSCE, Bangalore	ACSCE, Bangalore	ACSCE, Bangalore

Name of the Examiner	Signature with Date
_____	_____
_____	_____

ACS COLLEGE OF ENGINEERING

KAMBIPURA, MYSORE ROAD, BANGLORE-74

Department of Computer Science and Engineering

DECLARATION

We, **Mr. Vishal Prasad Sharma(1AH21CS123), Mr. Anayat Altaf Shah (1AH21CS127), Mr. Raj Kumar (1AH21CS081) and Mr. Vandan Kumar M (1AH21CS117)**, hereby declare that the project work entitled **"Blockchain Based Certificate Verification System"** has been independently carried out by us under the guidance of **Mr. Panchaxari Mamadapur**, Asst Prof, Department of Computer Science & Engineering, ACS College of Engineering, Bangalore, in partial fulfillment of the requirements of the degree of Bachelor of Engineering in Computer Science & Engineering of Visvesvaraya Technological University, Belgaum.

We further declare that we have not submitted this report either in part of in full to any other university for the reward of any degree.

Place: Bengaluru

Date:

Vishal Prasad Sharma(1AH21CS123)

Anayat Altaf Shah(1AH21CS127)

Raj Kumar(1AH21CS081)

Vandan Kumar M(1AH21CS117)

ACKNOWLEDGEMENT

I take this opportunity to express my sincere gratitude and respect to the **ACS College of Engineering**, Bengaluru for providing me an opportunity to carry out Internship report.

I express my deep regards to my honorable chairman **Sri Dr. A.C. Shanmugam** for providing me an opportunity to fulfil my ambition in this prestige institute.

I would like to express my immense gratitude to **Dr. Anandthirtha.B. Gudi**, Principal, ACS College of Engineering, Bengaluru, for his timely help and inspiration during the tenure of the course.

I express my sincere regards and thanks to **Dr. T Senthil Kumaran,** Professor & HOD, Computer Science and Engineering, ACSCE, Bengaluru for the encouragement and support throughout the work.

I hereby like to thank our Project Coordinator express **Ms. Lakshmi Priya P,** Assistant Professor, Computer Science and Engineering, ACSCE, Bengaluru for the encouragement and support throughout the work.

I am highly thankful to our guide **Mr. Panchaxari Mamadapur,** Assistant Professor, Computer Science and Engineering, ACSCE, Bengaluru for giving me a valuable suggestion, providing cooperation and moral support towards completion of Project Work.

Vishal Prasad Sharma(1AH21CS123)

Anayat Altaf Shah(1AH21CS127)

Raj Kumar(1AH21CS081)

Vandan Kumar M(1AH21CS117)

ABSTRACT

The proliferation of digital certificates and credentials has given rise to concerns surrounding authenticity, fraud, and the complexities of manual verification processes. Traditional centralized systems are vulnerable to single points of failure, data tampering, and lack of transparency. This application proposes a blockchain-based solution to address these challenges by leveraging the immutable, decentralized, and transparent nature of distributed ledger technology.

The proposed system comprises three main components: a user-friendly interface for certificate submission, integration with a blockchain network for secure data storage and hash generation, and a web page dedicated to certificate verification. Users can submit their digital certificates and relevant details through an intuitive interface, which generates a unique cryptographic hash value representing the certificate's contents.

This hash value is recorded on a blockchain network, ensuring its immutability and resistance to tampering. To facilitate efficient verification, the hash value is encoded into a QR code associated with the certificate. During the verification process, users can scan or upload the QR code, which is decoded to extract the hash value. The system queries the blockchain to retrieve the recorded hash and compares it with the extracted value. If the hash values match, the certificate is deemed authentic and valid. However, if a mismatch occurs, it indicates potential tampering, and the certificate is flagged as invalid.

The system adheres to security, performance, and usability best practices, ensuring a seamless user experience. It is designed to be scalable, interoperable, and promotes broader adoption across educational institutions and professional organizations globally. By leveraging blockchain's inherent advantages, this system establishes a trusted, transparent, and tamper evident framework for digital certificate verification, reducing fraud and enhancing the credibility of academic and professional credentials.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Overview

Blockchain technology has emerged as a revolutionary force, disrupting various industries and offering unprecedented levels of transparency, security, and decentralization. In the realm of digital certificates, blockchain-based verification systems have gained significant traction, addressing long-standing challenges like fraud, counterfeiting, and authenticity concerns. Traditional methods of issuing and verifying certificates often rely on centralized databases, which are susceptible to hacking, complex verification processes, and human error. These limitations necessitate a more secure, efficient, and trustworthy system—one that blockchain technology can provide.

A blockchain-based certificate verification system leverages the strengths of distributed ledger technology to ensure the immutability and transparency of recorded data. Each digital certificate is assigned a unique hash value, serving as a digital fingerprint that captures the certificate's content and metadata. This hash value is then stored on the blockchain, making any attempt to alter or tamper with the certificate immediately detectable through a mismatch of hash values.

The decentralized nature of blockchain eliminates the need for a central authority, reducing the risk of a single point of failure and enhancing overall system security. Furthermore, the integration of QR codes into the verification process simplifies accessibility and usability. By scanning a QR code associated with a certificate, users can seamlessly initiate the verification process, comparing the stored hash with the current certificate's hash to confirm its authenticity.

1.2 Areas of the Project

- Certificate Issuance: Generating unique digital certificates with metadata and content.
- Hashing Process: Creating a unique hash value for each certificate.
- Blockchain Integration: Storing the hash value on a decentralized blockchain network.
- QR Code Generation: Encoding the hash value into a QR code.

- Verification System: Matching the current certificate's hash with the stored hash.
- User Interface: Providing an accessible and user-friendly platform for verification.

1.3 Challenges and Complexities in the Project

- Ensuring data immutability and integrity.
- Managing efficient and scalable blockchain storage.
- Implementing fast and accurate hash comparisons.
- Simplifying the verification process for non-technical users.
- Addressing potential blockchain network fees and transaction speeds.
- Maintaining security while ensuring ease of use.

1.4 Motivation

The increasing prevalence of fraudulent certificates and the complexities of traditional verification methods highlight the need for a more secure and efficient system. Blockchain's ability to provide a decentralized, tamper-proof ledger offers a compelling solution to these issues. By integrating QR codes and user-friendly interfaces, this project aims to simplify and streamline certificate verification while maintaining high levels of security and trust.

1.5 Objectives

- Develop a blockchain-based certificate verification system.
- Ensure the authenticity and integrity of digital certificates.
- Eliminate the risk of centralized database vulnerabilities.
- Provide a simple, accessible verification process via QR codes.
- Enhance security, transparency, and efficiency.

1.6 Problem Statement

Traditional digital certificate verification systems suffer from security vulnerabilities, centralized points of failure, and complex verification processes. This project aims to

develop a blockchain-based system that ensures the authenticity, integrity, and transparency of digital certificates while simplifying the verification process.

1.7 Applications

- Educational institutions issuing degrees and certifications.
- Professional organizations providing accreditations.
- Government agencies verifying official documents.
- Corporate HR departments validating employee credentials.

1.8 Summary

Blockchain-based certificate verification systems offer a robust framework for establishing trust, transparency, and authenticity in digital credentials. By leveraging distributed ledger technology, unique hash values, and QR code integration, this approach enhances security, simplifies the verification process, and reduces the risk of fraud and counterfeiting.

CHAPTER 2

LITERATURE SURVEY

2.1 Introduction

Blockchain technology has a wide range of applications across various fields, including education, engineering, administration, medicine, elections, construction, and e-government. This research primarily focuses on the education sector, where blockchain is being increasingly adopted to address challenges related to certificate verification, fraud prevention, and data integrity. This section reviews existing research and case studies that highlight the use of blockchain technology in the education domain.

2.2 Background Study

In the 21st century, the rapid production of data across industries has introduced challenges in data collection, storage, and analysis. Blockchain technology, with its decentralized and immutable nature, offers a robust solution to these challenges. In the education sector, blockchain is being used to issue and verify academic credentials, digital badges, and certifications, ensuring transparency and reducing the risk of fraud.

2.3 Existing Model

1. European Data Science Academy (EDSA):

- EDSA utilizes blockchain technology to provide data science skills and certifications to job seekers.
- It also offers training programs to develop a new generation of world-leading data scientists.
- The system addresses challenges related to data collection, storage, and analysis in the digital age.

2. Certificate Validation Using Blockchain (Gayathiri et al., 2023):

- This paper proposes a blockchain-based system for certificate validation to address issues like certificate forgery and manual verification challenges.

- It highlights the immutable and decentralized nature of blockchains, which ensures transparency and tamper-resistance.

3. Award Badging and Validation Method (Fouzia et al., 2024):

- Focuses on using blockchain for validating digital badges or micro-credentials awarded for skills, achievements, or certifications.
- Argues that blockchain transparency can overcome challenges in traditional badging systems, such as centralization and lack of trusted verification.

4. Blockchain-Based Certificate Verification (Min Choi et al.):

- The system generates an electronic file of a paper certificate and calculates its hash value.
- The hash value is stored in the blockchain, and a QR code is generated for verification.
- Users can verify the authenticity of the certificate through mobile phone scanning or website inquiries.
- The unmodifiable properties of blockchain enhance the credibility of certificates and reduce the risk of loss or tampering.

5. Blockchain Internals and Digital Signatures (Hongning Dai et al.):

- Explains the structure of blockchain, including blocks, hashes, and the genesis block.
- Describes the use of private and public keys for signing and verifying transactions.
- Highlights the two phases of digital signatures: signing and verification.

6. Digitalization of Certificates (Gayatri et al.):

- Discusses the challenges faced by students and institutions in maintaining and validating academic certificates.
- Proposes a blockchain-based system to store certificates securely.

- Uses a chaotic algorithm to generate hash values for certificates, which are then stored on the blockchain.

7. Microsoft Certification Badges:

- Microsoft partnered with Pearson VUE's Acclaim platform to issue blockchain-based certification badges.
- These badges provide detailed information about the certification holder's skills and achievements.
- Benefits include easy sharing of certifications, identification of job opportunities, and salary expectations based on certified skills.

2.4 Summary

The literature survey highlights the growing adoption of blockchain technology in the education sector to address challenges related to certificate verification, fraud prevention, and data integrity. Existing models demonstrate the effectiveness of blockchain in ensuring transparency, immutability, and security in the issuance and validation of digital credentials. These systems leverage cryptographic hashing, QR codes, and decentralized ledgers to provide tamper-proof and user-friendly solutions for certificate management and verification.

CHAPTER 3

REQUIREMENT ANALYSIS

3.1 Introduction

The requirement analysis phase is crucial for understanding the scope, functionality, and constraints of the **Blockchain-Based Certificate Verification System**. This system is designed as a **standalone desktop application** that enables secure, tamper-proof issuance, verification, and management of educational certificates using blockchain technology. The application ensures data integrity, security, and ease of access without requiring an internet connection.

The system provides three core functionalities:

- **Certificate Issuance and Registration:** Securely issue and register certificates on the blockchain.
- **Certificate Verification:** Allow users to verify certificate authenticity through manual input or QR code scanning.
- **Certificate Management and Revocation:** Enable authorized institutions to manage and update certificate records when necessary.

This chapter outlines the system's **hardware and software requirements**, **performance expectations**, and **design constraints** to ensure the development of a robust and efficient application.

3.2 System Requirements

3.2.1 Hardware Requirements

- **Processor:** Intel Core i3 or higher
- **Memory:** Minimum 4GB RAM (recommended for optimal performance)
- **Storage:** Sufficient disk space for application and datasets

3.2.2 Software Requirements

- **Operating System:** Windows, macOS, Linux
- **Programming Language:** Python 3.9

- **Dependencies:**
    - **PyQt5:** For building the graphical user interface (GUI)
    - **Blockchain:** For creating data blocks and generating unique hash values
    - **QRCode:** For generating QR codes associated with hash values

3.3 Summary

This chapter describes the essential hardware and software requirements for the **Blockchain-Based Certificate Verification System**. The system is designed for cross-platform compatibility and provides a user-friendly interface for secure certificate handling. It leverages blockchain technology to ensure data security and integrity, offering a scalable and efficient solution for certificate management.

CHAPTER 4

PROPOSED SYSTEM

4.1 Introduction

The proposed system is a blockchain-based certificate verification system designed to address the challenges of fraud, counterfeiting, and inefficiencies in traditional certificate verification methods. By leveraging blockchain technology, the system ensures the authenticity, integrity, and transparency of digital certificates. This chapter provides an overview of the proposed model, detailed descriptions of sub-modules, data flow diagrams, and sequence diagrams.

4.2 Proposed Model

The proposed model follows a **Model-View-Controller (MVC) architecture**, which separates the system into three interconnected components:

- **Model**: Handles data storage and blockchain integration.
- **View**: Manages the user interface for certificate submission and verification.
- **Controller**: Implements the application logic, including hash generation, QR code creation, and verification processes.

The system integrates blockchain technology to generate unique cryptographic hash values for certificates, which are stored on an immutable distributed ledger. QR codes are used to encode these hash values, enabling seamless verification through scanning.

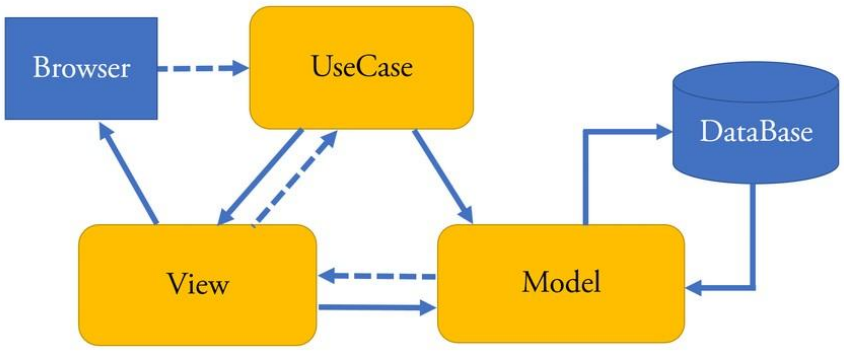

Fig 4.1: MVC Model

4.3 Detailed Description of Sub Models

4.3.1 Pre-Processing Module

- **Description**: Collects and validates certificate details and metadata from users.
- **Functionality**:
    - Accepts user inputs such as name, institution, degree, and year of graduation.
    - Validates input data to ensure accuracy and completeness.
    - Converts paper certificates into digital formats for processing.

4.3.2 Feature Extraction Module

- **Description**: Generates a unique cryptographic hash value for each certificate.
- **Functionality**:
    - Uses cryptographic algorithms (e.g., SHA-256) to generate hash values from certificate data.
    - Records the hash value on the blockchain network for immutability and transparency.

4.3.3 Classification

- **Description**: Converts hash values into QR codes for easy verification.
- **Functionality**:
    - Integrates a QR code generation library (e.g., qrcode) to create QR codes.
    - Associates the QR code with the corresponding certificate for future verification.

4.3.4 Training and Validation

- **Description**: Implements the verification process to validate certificate authenticity.
- **Functionality**:
    - Scans the QR code to extract the encoded hash value.

- Queries the blockchain network to retrieve the recorded hash value.
- Compares the hash value with the recorded value to determine authenticity.
- Displays the verification result to the user (authentic or tampered).

4.4 Data Flow Diagram (DFD)

4.4.1 Level 0 DFD

- **Overview**: Shows the interaction between users, the application, and the blockchain network.
- **Components**:
  - User: Submits certificate details and scans QR codes for verification.
  - Application: Processes data, generates hash values, and interacts with the blockchain.
  - Blockchain Network: Stores hash values and provides verification results.

4.4.2 Level 1 DFD

- **Detailed Flow**: Illustrates the steps in certificate issuance and verification.
  - Certificate Issuance: User submits certificate details → Hash value generated → Hash value stored on blockchain → QR code generated.
  - Certificate Verification: User scans QR code → Hash value extracted → Blockchain queried → Hash values compared → Verification results displayed.

4.4.3 Level 2 DFD

- **Specific Steps**: Breaks down the verification process into finer details.
  - QR Code Scanning: Captures QR code image → Decodes hash value.
  - Blockchain Query: Retrieves recorded hash value based on certificate details.
  - Comparison: Compares extracted and recorded hash values.
  - Result Display: Shows "Authentic" or "Tampered" based on comparison.

4.5 Sequence Diagram

- **Description**: Illustrates the sequence of interactions between system components during certificate issuance and verification.
- **Steps**:
    1. User submits certificate details.
    2. Application generates hash value and stores it on the blockchain.
    3. Application generates a QR code for the certificate.
    4. User scans the QR code for verification.
    5. Application decodes the QR code and queries the blockchain.
    6. Application compares hash values and displays the result.

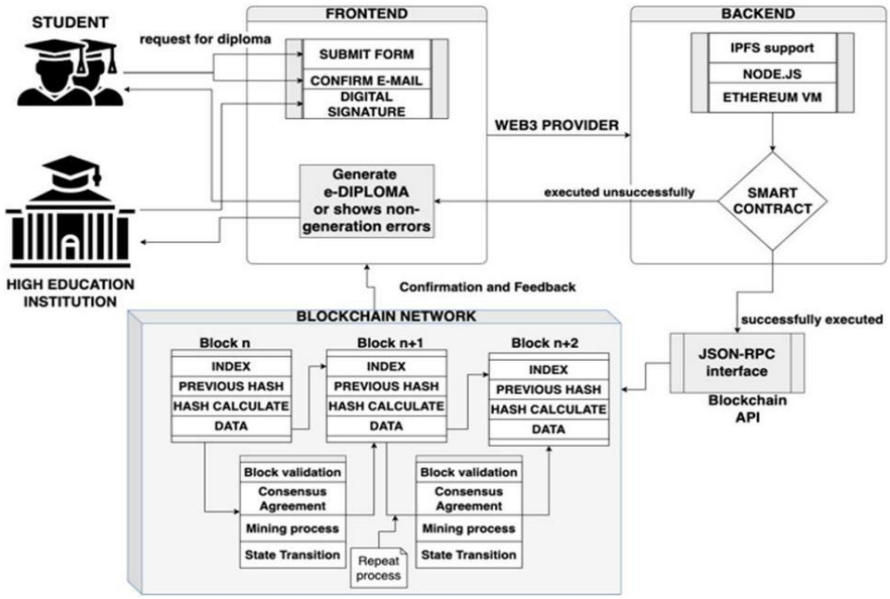

Fig 4.2: Dataflow diagram

4.6 Summary

The proposed system leverages blockchain technology and QR codes to provide a secure, transparent, and user-friendly solution for certificate verification. It addresses the limitations of traditional methods by ensuring the authenticity and integrity of digital credentials. The system is designed to be scalable, interoperable, and accessible to a wide range of users, including educational institutions, professional organizations, and regulatory bodies.

CHAPTER 5

IMPLEMENTATION

5.1 Introduction

The implementation phase is the practical realization of the system architecture and design principles defined in earlier stages. In this project, the implementation brings to life a Blockchain-Based Certificate Verification System, aiming to resolve issues related to digital certificate authenticity, security, and efficiency. This system combines multiple components—certificate data handling, hash generation, QR code integration, blockchain entry, and verification—into a desktop-based application built using Python. The goal is to create a user-friendly interface that communicates with backend logic and a simulated blockchain to securely process and verify educational or professional certificates.

5.2 Implementation

Programming Language and Platform

The system is implemented using **Python 3.9**, a high-level, general-purpose language known for its simplicity, wide library support, and versatility. Python is particularly suitable for prototyping and developing applications involving GUI development, cryptographic operations, and data processing.

The platform chosen is a **desktop application**, developed and tested on **Windows 10** using **Visual Studio Code (VS Code)**. A desktop-based system provides better offline accessibility and performance while allowing closer integration with system resources. This implementation ensures cross-platform compatibility, allowing the system to be extended to Linux and macOS with minimal modifications.

Libraries and Tools Used

The following Python libraries were integral to the implementation:

- **PyQt5**: Used for creating the graphical user interface (GUI) where users interact with the system to submit, view, and verify certificates.
- **hashlib**: Generates cryptographic hashes (SHA-256) for certificate data, ensuring integrity and tamper detection.
- **QRCode**: Converts the generated hash values into scannable QR codes that are associated with certificates.

- **pandas**: Supports data handling and file I/O operations.
- **Custom blockchain module**: Simulates the creation of a blockchain by generating blocks and storing hashes linked to prior blocks.

Code Structure and Conventions

To ensure modularity and maintainability:

- Variables and functions are named using snake_case
- Classes are named using UpperCamelCase
- Each functionality is modularized into separate Python files:
    - hash_value.py for hash generation
    - qrcode_generator.py for QR code creation
    - blockchain.py for block generation and verification
    - main.py (or similar) for GUI interactions

Modules are documented with appropriate comments and docstrings, and error handling is incorporated to ensure robustness.

Architecture and Workflow

The system follows a **Model-View-Controller (MVC)** design pattern to separate the data layer, business logic, and interface:

- **Model**: Includes certificate data structures and blockchain logic.
- **View**: The PyQt5-based GUI that provides input forms, QR display windows, and feedback messages.
- **Controller**: Bridges the interface with the logic, handling input, generating hashes, storing them on the blockchain, and managing the verification logic.

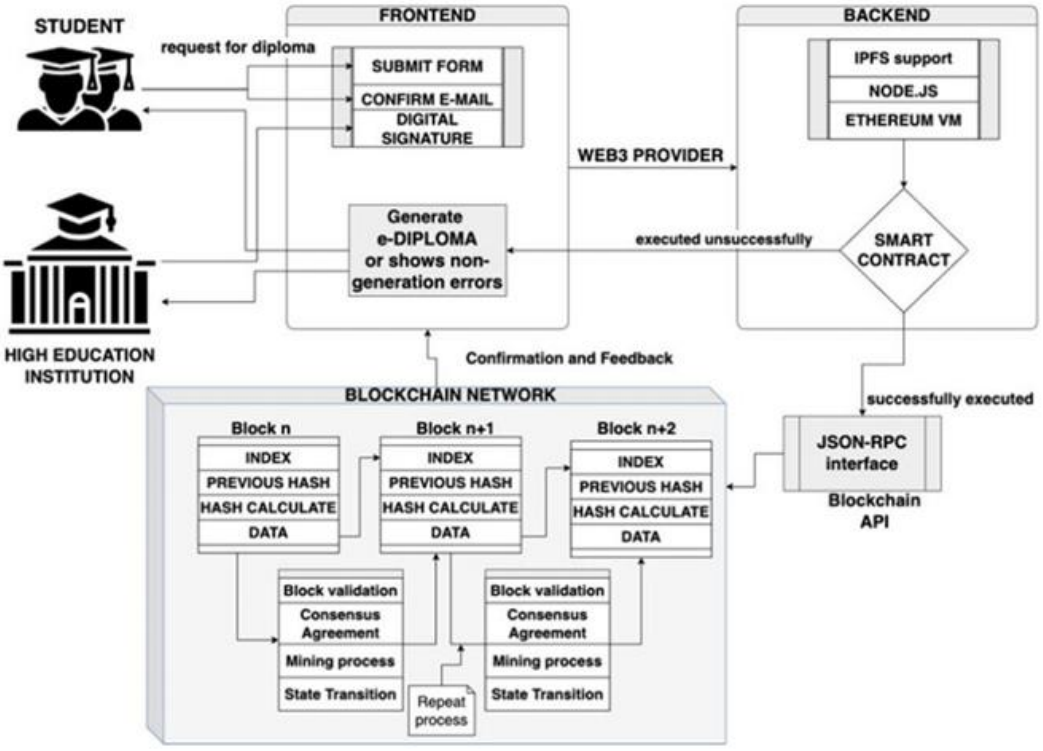

Fig 5.1: Implementation

This figure illustrates the functional flow: certificate data is submitted via the GUI, hashed, stored on a blockchain, converted into a QR code, and later verified by decoding and comparing the hash.

Module-Level Implementation

Certificate Module

This module handles the input and storage of student or user information. It takes inputs such as name, institution, degree, and graduation year, and stores them in a structured format for further processing.

Hashing Module

Uses the hashlib library to generate a secure hash using the SHA-256 algorithm. This hash serves as a unique digital fingerprint for the certificate, ensuring immutability and authenticity.

Blockchain Module

Implements a simulated blockchain structure using text files. Each new certificate entry is stored as a block that includes the current hash, timestamp, and a reference to the previous

block's hash. This chaining ensures that any tampering with a previous block invalidates the chain.

QR Code Module

The qrcode module generates a QR code image from the hash value. This QR code is then displayed on the interface and can be printed or stored digitally alongside the certificate.

Verification Module

This module allows users to scan or upload a QR code. The system extracts the hash value from the code, checks the blockchain for a matching entry, and returns a verification result (authentic or tampered).

Graphical User Interface (GUI)

The GUI is built with PyQt5 and features:

- A login page
- Certificate registration form
- QR code viewer
- Verification tool with scan/upload options

The interface is designed for ease of use, guiding users through each step of the process with labels, buttons, and messages.

5.3 Summary

This chapter has presented the step-by-step implementation of the Blockchain-Based Certificate Verification System. Python was chosen for its ease of use and strong ecosystem, and the desktop platform ensures performance and reliability. The MVC architecture enhances maintainability and logical separation of responsibilities. Each module—from certificate handling to blockchain entry and verification—was implemented with clarity and efficiency. The next chapter will evaluate the system through comprehensive testing and analyze its behavior in various operating scenarios.

CHAPTER 6

RESULTS

6.1 Introduction

This chapter presents the evaluation and analysis of the Blockchain-Based Certificate Verification System developed and implemented in the previous stages. The primary goal is to assess the functionality, performance, and correctness of the system through various levels of testing. These include unit testing of individual modules, integration testing of interconnected components, and system-level testing under both normal and adverse conditions. Furthermore, this chapter documents successful operational flows, worst-case scenarios, and non-functional cases to demonstrate the system's robustness. It also provides a comparative analysis against traditional systems to highlight improvements and limitations.

6.2 Result Analysis – Test Cases

The system was tested using structured test cases for each component and user interaction.

6.2.1 Unit Testing

Unit testing focused on verifying the correctness of individual components such as:

- **Hash Generation**: Ensuring consistent SHA-256 hash values for identical input data.
- **QR Code Creation**: Confirming that generated QR codes accurately represent their corresponding hash.
- **Blockchain Storage**: Testing the creation of new blocks, proper chaining via hash linkage, and timestamp validation.
- **GUI Actions**: Validating button clicks, data entry fields, and file upload functionalities.

The testing was conducted using Python's built-in unittest framework and pytest. Each method was tested with both valid and edge case inputs.

6.2.2 Integration Testing

Integration testing ensured that various modules interact seamlessly. The test cases validated:

- Data flow from GUI to the hash generator.
- Correct handoff of hash values to the blockchain module.
- QR code creation based on blockchain-stored hash values.
- Interaction between QR scanner and verifier logic.

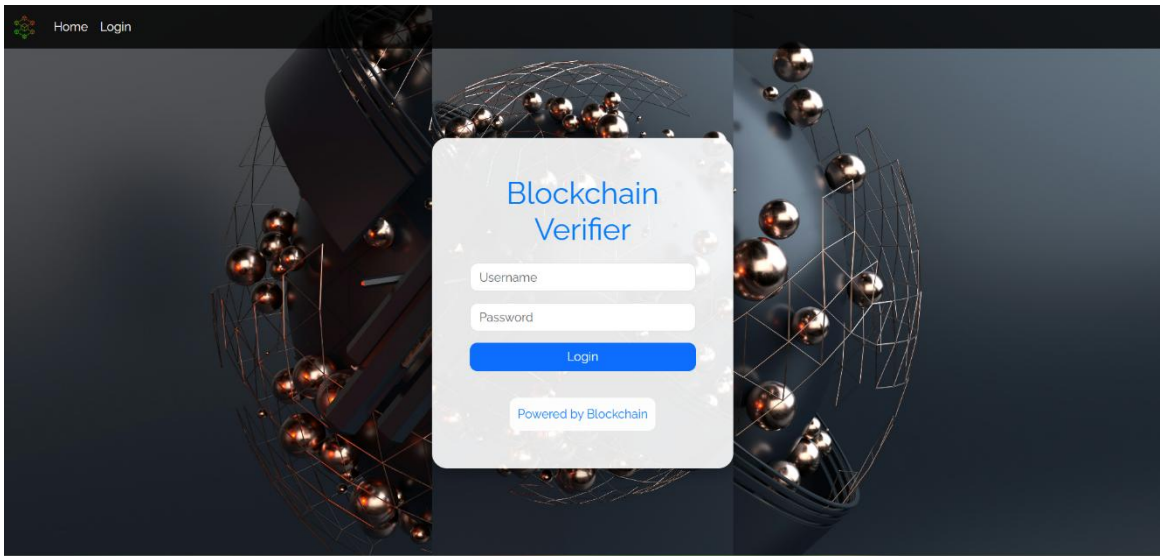

Fig 6.1: GUI Interface here to show the user login page.

GUI Interface – Displays the user login page where authorized users can securely access the system.

6.2.3 System Testing

System-level testing evaluated the entire workflow, starting from certificate entry to final verification. The steps tested include:

1. User enters certificate details and uploads the document.
2. The system generates a hash, creates a blockchain block, and generates a QR code.
3. The QR code is either saved or displayed to the user.
4. During verification, the QR code is scanned/uploaded.
5. The system retrieves the hash and compares it with the blockchain record to determine authenticity.

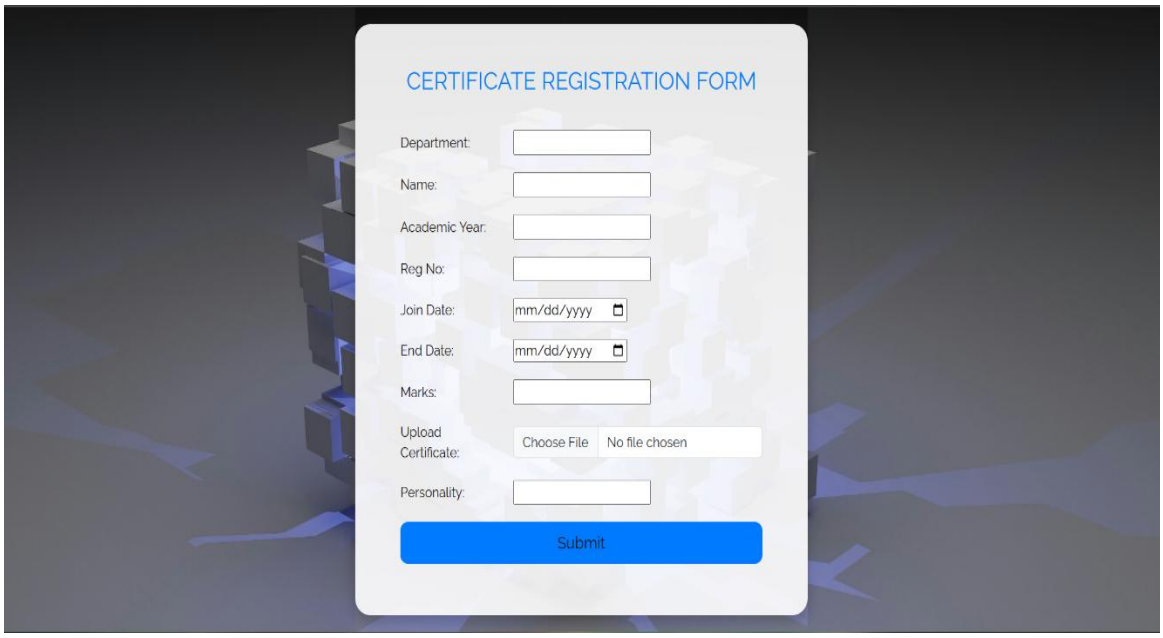

Fig 6.2: Certificate Registration where users input their information.

Certificate Registration – Shows the form where users input certificate details and upload documents for verification.

Fig 6.3: Generated QR Code here to show the hash represented as a QR code.

Generated QR Code – Depicts the QR code generated from the certificate's hash, which can later be scanned for verification.

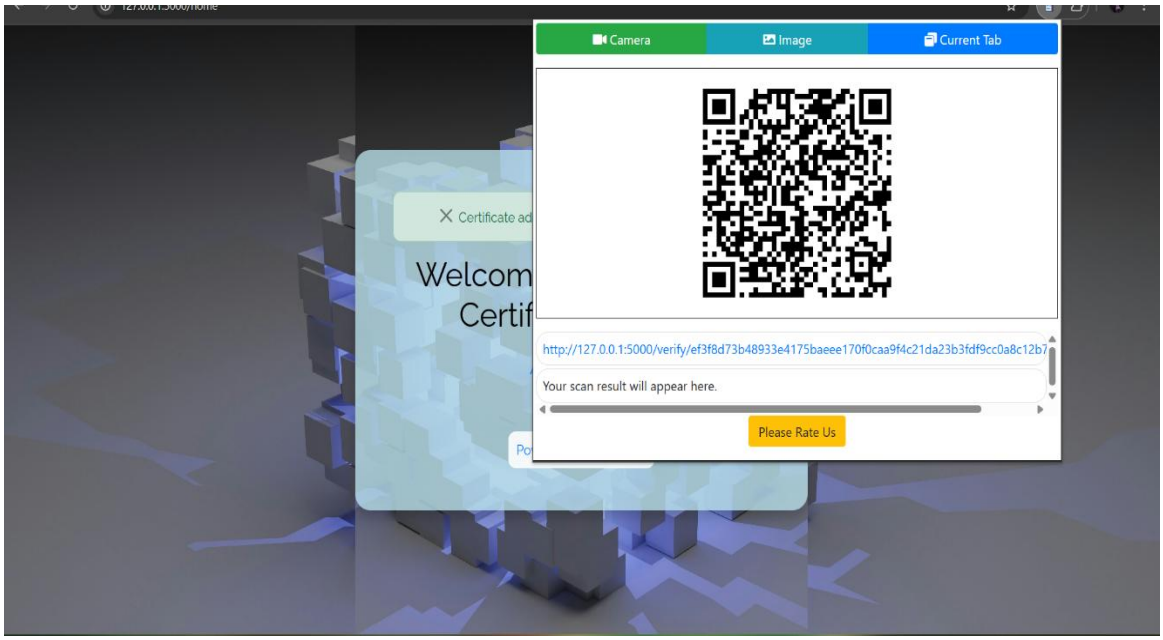

Fig 6.4: QR Code Scanner to show the verification process in progress.

QR Code Scanner – Illustrates the scanning interface used to read the QR code and initiate certificate verification

6.3 Working Case

In the best-case scenario, a valid certificate is uploaded and processed, and the system generates the correct hash, stores it on the blockchain, and creates a valid QR code. When the QR code is scanned, the system accurately verifies and displays a message indicating that the certificate is authentic.

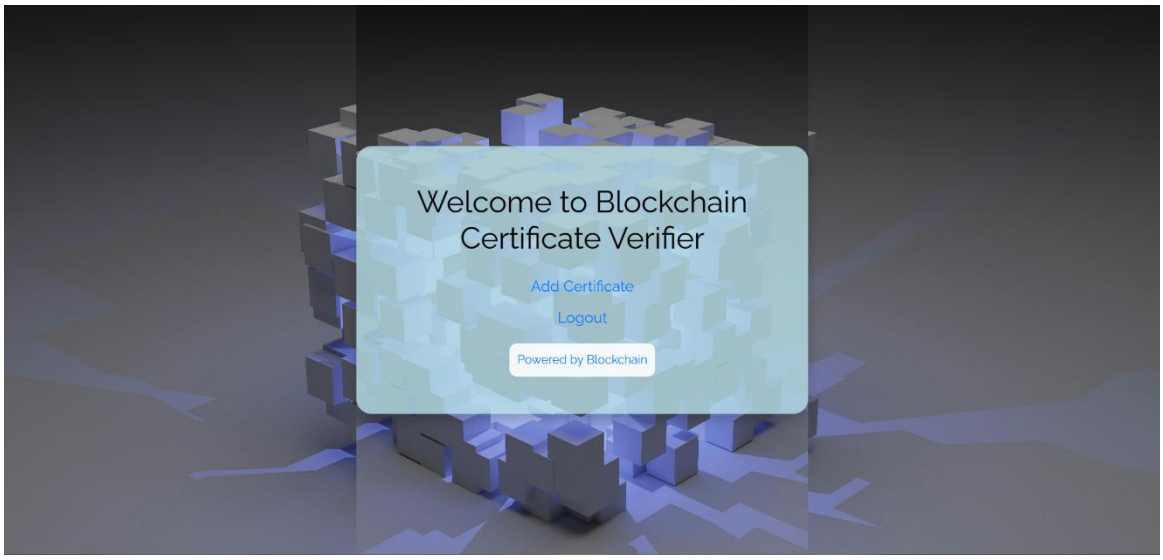

Fig 6.5: To Add Certificate

To Add Certificate – Represents the interface used to add a new certificate to the blockchain system.

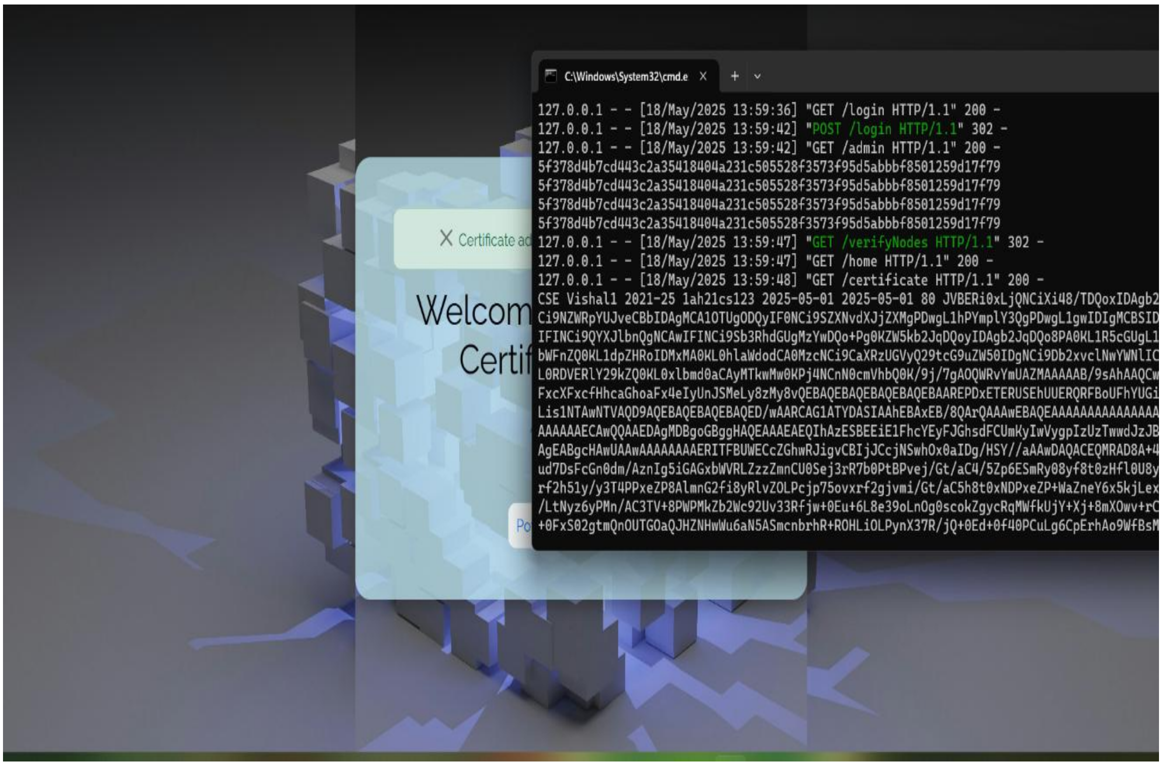

Fig 6.6: Block Created after adding Certificate

Block Created – Visualizes a newly created block in the blockchain containing the certificate's hash and metadata.

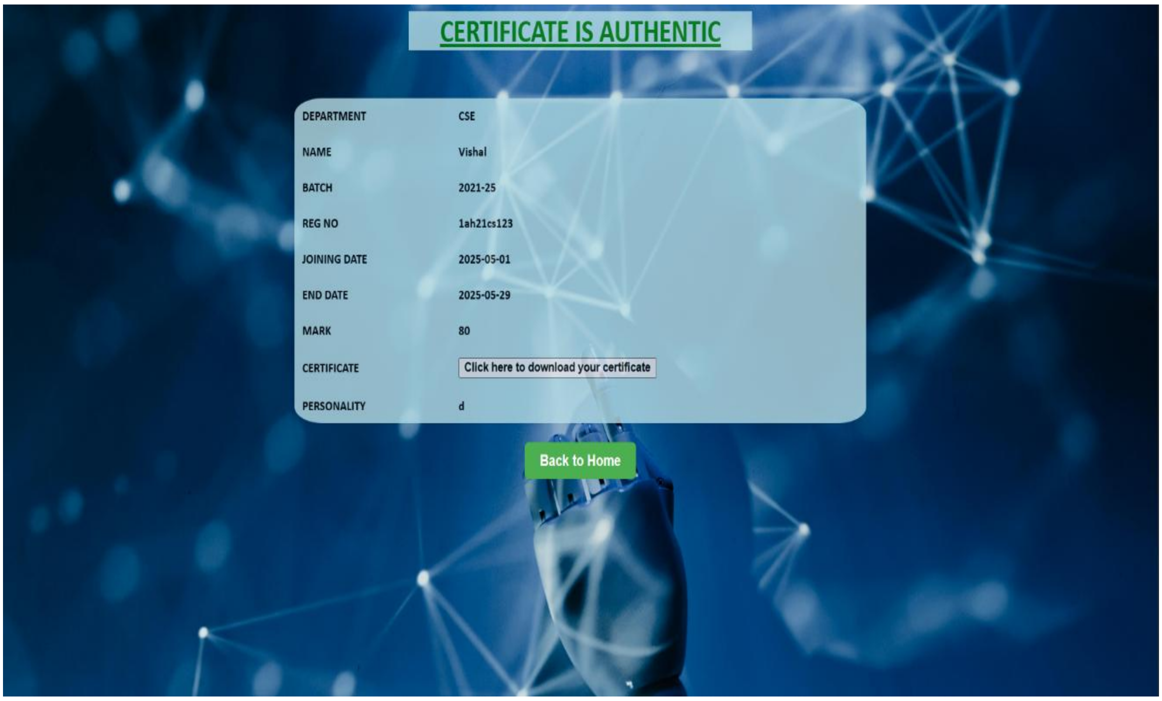

Fig 6.7: After Verification of Authentic Certificate

After Verification of Authentic Certificate – Shows a success message confirming that the scanned certificate is valid and verified.

6.4 Not Working Case with Justification

Certain controlled test cases were designed to fail in order to validate the system's ability to detect and handle errors. Examples include:

- **Tampered QR Code**: If a QR code is altered manually or generated from a different hash, the system compares it with the blockchain and fails the verification process.
- **Missing Blockchain Entry**: If the hash in the QR code doesn't exist in the blockchain (e.g., QR generated from an external source), the system correctly flags it as invalid.

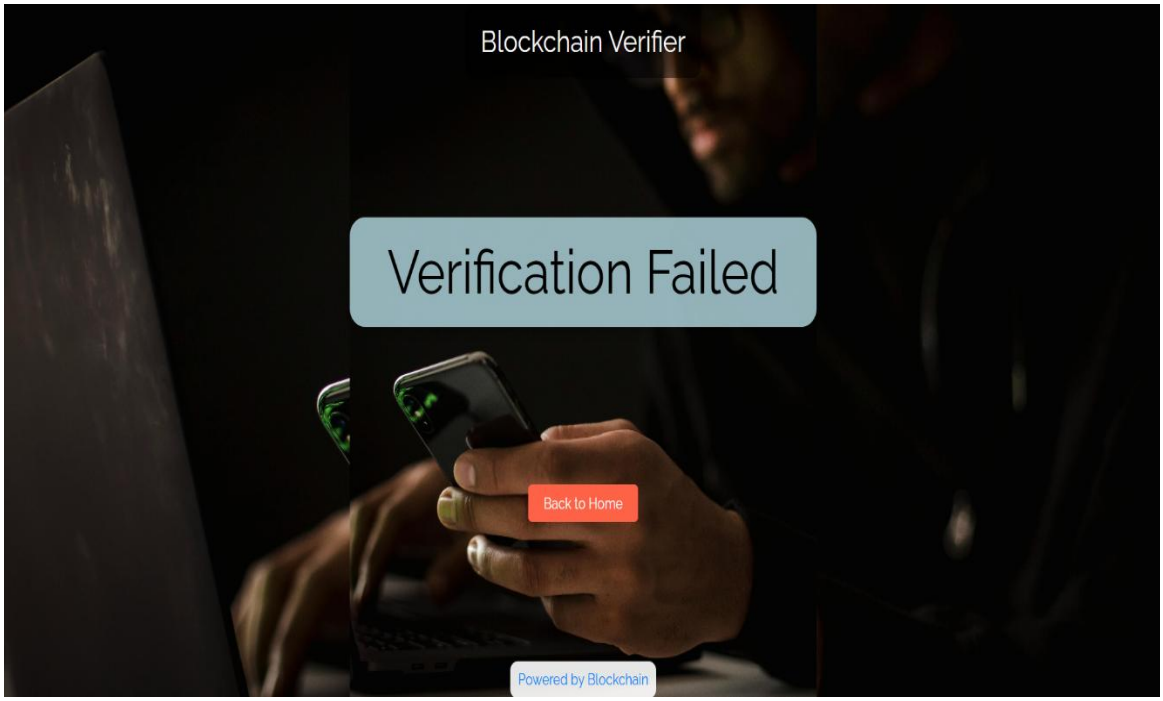

Fig 6.8: After Verification of Fake Certificate due to mismatch

After Verification of Fake Certificate – Displays a failure message triggered when the QR code does not match any blockchain record, indicating a tampered or invalid certificate.

These failure responses reinforce the system's security objective—ensuring only verifiable, non-tampered certificates are accepted.

6.5 Comparative Analysis

This section compares the blockchain-based system with traditional verification methods. This comparison shows that blockchain drastically improves reliability, speed, and resistance to fraud, making it a superior method for digital certificate validation.

Table 6.1 Comparision of Traditional System and Blockchain based System

Feature	Traditional System	Blockchain-Based System
Tamper Detection	Manual and limited	Cryptographically secured
Verification Time	Several days (manual)	Instant (via QR and hash check)
Dependency on Authority	High (centralized database)	Low (decentralized verification)
Accessibility	Requires human involvement	Fully automated and scalable
Data Integrity Assurance	Low	High (immutability via blockchain)

6.6 Summary

This chapter presented the outcome of testing and real-time performance of the Blockchain-Based Certificate Verification System. The system was subjected to unit, integration, and full system testing under various input conditions. Test results confirmed the correct functionality of all modules, robustness in handling edge cases, and high reliability in authenticating certificates. Both successful and failed verification scenarios were explored, with screenshots demonstrating real project outputs. Compared to traditional methods, this system showed notable improvements in speed, accuracy, and security.

CHAPTER 7

CONCLUSION

In conclusion, while blockchain-based certificate verification systems offer transparency, immutability, and decentralization, they face challenges like scalability, privacy concerns, and adoption barriers. Future enhancements focus on improving scalability, implementing privacy preserving techniques, establishing interoperability standards, adopting sustainable consensus mechanisms, enhancing user experience, integrating with emerging technologies, and ensuring regulatory compliance. Addressing these limitations and capitalizing on potential enhancements will drive the widespread adoption and effectiveness of these systems. Through ongoing development, collaboration, and feedback, we aim to create a robust and user-friendly software solution that delivers value and facilitates learning and exploration in various domains.

7.1 Limitations

1. Scalability: Blockchain technology has scalability challenges, particularly when dealing with a large volume of transactions or data. As the number of certificates and verifications increases, the network may face performance issues and slower transaction processing times.

2. Privacy and Data Protection: While blockchain provides transparency, there are concerns about the privacy of personal and sensitive information stored on a public ledger. Appropriate measures must be taken to protect individuals' privacy and comply with data protection regulations.

3. Adoption and Interoperability: Widespread adoption and interoperability among different organizations and industries can be challenging. Standardization and common protocols are necessary to ensure seamless integration and acceptance of blockchain-based certificate verification systems.

4. Energy Consumption: Some blockchain consensus mechanisms, like Proof-of-Work (PoW), are energy-intensive and may not align with sustainability goals. Alternative consensus mechanisms, such as Proof-of-Stake (PoS), can help mitigate this issue.

5. User Experience: Blockchain technology can be complex for end-users, requiring additional training and education to ensure proper usage and understanding of the certificate verification process.

7.2 Future Enhancements

1. Improved Scalability: Ongoing research and development in blockchain technology aim to address scalability concerns through solutions like sharding, off-chain computations, and layer-2 scaling solutions.

2. Privacy-Preserving Techniques: Advancements in cryptographic techniques, such as zero knowledge proofs and secure multi-party computation, can enhance privacy while maintaining transparency and verification capabilities.

3. Interoperability Standards: The development of industry-wide standards and protocols for blockchain-based certificate verification systems can facilitate seamless integration and cross organizational collaboration.

4. Sustainable Consensus Mechanisms: Continued research and adoption of energy-efficient consensus mechanisms, like Proof-of-Stake (PoS) or novel mechanisms, can contribute to the sustainability and environmental friendliness of blockchain solutions.

5. User Experience Improvements: Simplified user interfaces, educational resources, and user-friendly tools can enhance the accessibility and adoption of blockchain-based certificate verification systems for various stakeholders.

6. Integration with Emerging Technologies: Exploring the integration of blockchain with other emerging technologies, such as the Internet of Things (IoT), artificial intelligence (AI), and digital identities, can unlock new possibilities and use cases for certificate verification and authentication.

7. Regulatory Compliance: Ongoing collaboration with regulatory bodies and policymakers can ensure that blockchain-based certificate verification systems comply with relevant laws and regulations, facilitating broader adoption and trust.

REFERENCES

[1] D. A.Gayathiri, J.Jayachitra (2022). Certificate validation using blockchain. 7th International Conference on Smart Structures and Systems ICSSS 2020, 8, 34929 – 34941.

[2] A. S. P. A. Fouzia F. Ozair, Nayer Jamshed (2021). "Award badging and validation method using blockchain". Proceedings of the Second International Conference on Inventive Research in Computing Applications, 315 – 323.

[3] J. Y. H. Hyunil kim, Seuign-Hyun Kim and C. Seo (2020). How to timestamp a digital document. 1991 International Association for Cryptologic Research.

[4] C. C. Jilin-Chiou Cheng, Narn-Yih Lee and Y.-H. Chen (2021). "Block-chain and smart contract for digital certificate". Proceedings of the Fifth International Conference on Intelligent Computing and Control Systems (ICICCS 2021), 9, 106790 – 106805.

[5] H. D. X. C. Zibin Zheng, Shaoan Xie1 and H. Wang (2019). "Block-chain technology consensus and future trend". 7, 41525 – 41550.

[6] Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: a perspective from blockchain technology. Financial Innovation, 2(1), 1-10.

[7] Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. Smart Learning Environments, 5(1), 1-10.

[8] Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C. F., & Wendland, F. (2018, September). Blockchain for education: lifelong learning passport. In Proceedings of 1st ERCIM Blockchain Workshop 2018 (pp. 1-10). European Society for Socially Embedded Technologies (SSEP).

[9] Haq, I. U., Muselemu, O. E., & Shoaib, M. (2019). Blockchain technology applications challenges and future perspective. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 11(2), 121-125.

[10] Sayed, A. E. R. M., & AlSayah, M. (2019, March). Blockchain certificate verification system. In 2019 IEEE International Conference on Multimedia & Expo Workshops (ICMEW) (pp. 477 482). IEEE.

[11] Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. IEEE Access, 6, 5112-5127.

[12] Wang, F., & De Filippi, P. (2020). Self-sovereign identity in a globalized world: Credentials based identity systems as a driver for economic inclusion. Frontiers in Blockchain, 2, 28.

[13] Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C. F., & Wendland, F. (2018, September). Blockchain for education: lifelong learning passport. In Proceedings of 1st ERCIM Blockchain Workshop 2018 (pp. 1-10). European Society for Socially Embedded Technologies (SSEP).

[14] Sharples, M., & Domingue, J. (2016). The blockchain and kudos: A distributed system for educational record, reputation and reward. In K. Verbert, M. Sharples, & T. Klobučar (Eds.), Adaptive and Adaptable Learning (pp. 490-496).

[15] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

[16] Grech, A., & Camilleri, A. F. (2017). Blockchain in education. Publications Office of the European Union.

[17] Chenward, G., Xu, B., Lu, M., & Chen, N. S. (2019). Exploring blockchain technology and its potential applications for education. Smart Learning Environments, 5(1), 1-10.

[18] Srivastava, G., Dwivedi, A. D., & Singh, R. (2021). Blockchain education: A systematic literature review. Archives of Computational Methods in Engineering, 1-22.

[19] Rimol, M. (2018, June). Blockcerts academic credentials on the Bitcoin blockchain. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems (pp. 46-53).

[20] Xiong, H., Dai, X., Bajaj, J., & Kashti, A. (2020, August). Certchain: A blockchain-based framework for education system. In 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC) (pp. 1039-1048). IEEE.