# BLOCKCHAIN-BASED CERTIFICATE VALIDATION

## A PROJECT REPORT

***Submitted by,***

# Mr. Maddi Shanmukha Mahesh Babu - 20201CCS0016 Mr. Nagubandi Viswesh -20201CCS0091 Mr. Lakku Rohith Kumar Reddy -20201CCS0125

***Under the guidance of,* Dr. Syed Siraj Ahmed Associate Professor**

***in partial fulfillment for the award of the degree of***

# BACHELOR OF TECHNOLOGY

## IN

**COMPUTER SCIENCE AND ENGINEERING(CYBER SECURITY)**

**At**



# PRESIDENCY UNIVERSITY BENGALURU JANUARY 2024

**PRESIDENCY UNIVERSITY**

**SCHOOL OF COMPUTER SCIENCE ENGINEERING**

# CERTIFICATE

This is to certify that the Project report **“BLOCK-CHAIN BASED CERTIFICATE VALIDATION”** being submitted by “Maddi Shanmukha Mahesh Babu”, “Nagubandi Viswesh”, “Lakku Rohith Kumar Reddy” bearing roll number(s) “20201CCS0016”, “20201CCS0091”, “20201CCS0125” in

partial fulfilment of requirement for the award of degree of Bachelor of Technology in Computer Science and Engineering (Cyber Security) is a bonafide work carried out under my supervision.

|  |  |
| --- | --- |
| **Dr. Syed Siraj Ahmed** Associate Professor School of CSE&IS  Presidency University | **Dr. Anandaraj S P** & Professor & HOD, School of CSE&IS  Presidency University |

|  |  |  |
| --- | --- | --- |
| **Dr. C. KALAIARASAN**  Associate Dean School of CSE&IS Presidency University | **Dr. SHAKKEERA L**  Associate Dean School of CSE&IS Presidency University | **Dr. Md. SAMEERUDDIN KHAN**  Dean  School of CSE&IS Presidency University |

**PRESIDENCY UNIVERSITY**

# SCHOOL OF COMPUTER SCIENCE ENGINEERING

**DECLARATION**

We hereby declare that the work, which is being presented in the project report entitled **Blockchain-Based Certificate Validation** in partial fulfilment for the award of Degree of **Bachelor of Technology** in **Computer Science and Engineering(Cyber Security)**, is a record of our own investigations carried under the guidance of **Dr. Syed Siraj Ahmed, Associate Professor, School of Computer Science Engineering, Presidency University, Bengaluru.**

We have not submitted the matter presented in this report anywhere for the award of any other Degree.

## Maddi Shanmukha Mahesh Babu, 20201CCS0016 Nagubandi Viswesh, 20201CCS0091

**Lakku Rohith Kumar Reddy,20201CCS0125**

**ABSTRACT**

Verifying and validating certificates is crucial in ensuring the legitimacy and authenticity of credentials provided by educational institutions, professional associations, and other organizations. Traditional methods of certificate verification sometimes include the use of centralized databases, which are vulnerable to fraud, manipulation, and unauthorized access. Recently, blockchain technology has surfaced as a viable means of improving the security and dependability of certificate verification processes. To begin the certificate verification process, a certificate is issued by an authorized body. In addition to being digitally signed and stored on the blockchain, the certificate also receives a distinct cryptographic hash that serves as its digital fingerprint. This hash is stored on the blockchain together with relevant metadata such as the issuer, receiver, issue date, and expiration. This report explores a blockchain-based certificate verification system that offers enhanced security and transparency. The system involves:

**Keywords:** Admin, Institutions, Scanner Module, Upload file, Scan QR code.

**ACKNOWLEDGMENT**

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected **Dr. Md. Sameeruddin Khan**, Dean, School of Computer Science Engineering & Information Science, Presidency University for getting us permission to undergo the project.

We record our heartfelt gratitude to our beloved Associate Deans **Dr. Kalaiarasan C and Dr. Shakkeera L,** School of Computer Science Engineering & Information Science, Presidency University and **Dr. S.P. Anandaraj**. Head of the Department, Computer Science Engineering (Cyber Security), Presidency University for rendering timely help for the successful completion of this project. We are greatly indebted to our guide **Dr. Syed Siraj Ahmed, Associate Professor**, School of Computer Science Engineering, Presidency University for his inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the project work.

We would like to convey our gratitude and heartfelt thanks to the University Project-II Coordinators **Dr. Sanjeev P Kaulgud, Dr. Mrutyunjaya MS** and also the department Project Coordinator **Ms. Manasa C M**.

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

## Maddi Shanmukha Mahesh Babu

**Nagubandi Viswesh Lakku Rohit Kumar Reddy**

**LIST OF TABLES**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl. No.** | **Table Name** | **Table Caption** | **Page No.** |
| 1 | Table 1 | Timeline of a Project | 48 |

**LIST OF FIGURES**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl. No.** | **Figure Name** | **Caption** | **Page No.** |
| 1 | Figure 1 | Block Diagram | 15 |
| 2 | Figure 2 | Architecture | 16 |
| 3 | Figure 3 | Use Case Diagram | 20 |
| 4 | Figure 4 | Class Diagram | 21 |
| 5 | Figure 5 | Sequence Diagram | 22 |
| 6 | Figure 6 | Activity Diagram | 23 |
| 7 | Figure 7 | Data Flow Diagram (level 0) | 24 |
| 8 | Figure 8 | Data Flow Diagram (level 1) | 24 |
| 9 | Figure 9 | Data Flow Diagram (level 2) | 25 |
| 10 | Figure 10 | Command | 26 |
| 11 | Figure 11 | Index | 26 |
| 12 | Figure 12 | Admin Login | 27 |
| 13 | Figure 13 | Admin Login Action | 27 |
| 14 | Figure 14 | Add Certificate | 28 |
| 15 | Figure 15 | Add Certificate Action | 28 |
| 16 | Figure 16 | Add Certificate Action | 29 |
| 17 | Figure 17 | View Certificate | 29 |
| 18 | Figure 18 | View Companies | 30 |
| 19 | Figure 19 | Signup | 30 |
| 20 | Figure 20 | Signup Action | 31 |
| 21 | Figure 21 | Login | 31 |
| 22 | Figure 22 | Login Action | 32 |
| 23 | Figure 23 | Authenticate Scan | 32 |
| 24 | Figure 24 | Authenticate Scan Action | 33 |
| 25 | Figure 25 | Authenticate Scan | 33 |
| 26 | Figure 26 | Authenticate Scan Action | 34 |
| 27 | Figure 27 | Web Cam Verification | 34 |
| 28 | Figure 28 | QR Code Scanner | 35 |
| 29 | Figure 29 | QR Code exists | 35 |
| 30 | Figure 30 | QR Code not exists | 36 |
| 31 | Figure 31 | Gantt Chart | 39 |

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
|  | **ABSTRACT ACKNOWLEDGMENT**  **LIST OF TABLES**  **LIST OF FIGURES** | **iv v vi**  **vii** |
| **1.** | **INTRODUCTION** | 1 |
|  | 1.1 Problem Statement | 1 |
|  | 1.2 Objective of the Project | 1 |
|  | 1.3 Scope | 2 |
|  | 1.4 Project Introduction | 2-3 |
| **2.** | **LITERATURE REVIEW** | **4** |
|  | 2.1 Related Work | 4-12 |

|  |  |  |
| --- | --- | --- |
| **3.** | **RESEARCH GAPS OF EXISTING METHODS** | 13 |
|  | 3.1 Existing System | 13 |
|  | 3.2 Disadvantages | 13 |

|  |  |  |
| --- | --- | --- |
| **4.** | **PROPOSED METHODOLOGY** | 14 |
|  | 4.1 Proposed System | 14 |
|  | 4,2 Advantages | 14 |
|  | 4.3 Block Diagram | 15 |
|  | 4.4 Architecture | 16 |

|  |  |  |
| --- | --- | --- |
| **5.** | **OBJECTIVES** | 17 |
|  | 5.1 Objectives | 17 |

|  |  |  |
| --- | --- | --- |
| **6** | **SYSTEM DESIGN & IMPLEMENTATION** | 18 |
|  | 6.1 Introduction of Input Design | 18 |
|  | 6.2 UML Diagram (use case, class, sequence, activity) | 18-22 |
|  | 6.3 Data Flow Diagram | 23-25 |
|  | 6.4 Output Screens | 25-36 |
|  | 6.5 About solidity Ethereum algorithm | 37-38 |
| **7.** | **TIMELINE FOR EXECUTION OF PROJECT** | 39 |
|  | 7.1 Timeline of project | 39 |
|  | 7.2 Gantt Chart | 39 |
| **8.** | **OUTCOMES** | 40 |
| **9.** | **RESULTS AND DISCUSSIONS** | 41 |
|  | **9.1 Results** | 41 |
|  | **9.2 Discussions** | 41 |

|  |  |  |
| --- | --- | --- |
| **10.** | **CONCLUSION** | 42 |
| **11.** | **REFERENCES** | 43 |
| **12.** | **APPENDIX-A (PSUEDOCODE)** | 44-46 |
| **13.** | **APPENDIX-B (SCREENSHOTS)** | 47-55 |
| **14.** | **APPENDIX-A (ENCLOSURES)** | 56-57 |

# CHAPTER-1 INTRODUCTION

## Problem Statement:

Conventional techniques for verifying certificates that rely on central databases are vulnerable to manipulation, fraud, and unapproved access. This makes verifying the legitimacy and authenticity of certificates from academic institutions and professional associations extremely difficult. Blockchain technology shows promise as a remedy for these problems. The technique provides tamper-proof verification by digitally signing and storing certificates on a blockchain, each with a distinct cryptographic hash. However the lack of a globally accepted and standardized blockchain-based certificate verification system now in place makes it difficult to build a technique that is both universally safe and trustworthy, which has an effect on the integrity of credential validation in a variety of industries and organizations.

## Objective of the Project:

The Objective of employing blockchain technology for certificate verification and validation is to utilize its intrinsic characteristics, including immutability, decentralization, and transparency, to establish a reliable and secure system for certificate verification and validation. The objectives are to lower dependency on centralized authorities, create a visible and auditable record of certificate transactions, remove the possibility of fraud and manipulation, expedite the verification process, and improve overall effectiveness and confidence in the certification ecosystem.

## Scope:

The scope of the project involves implementing a secure and tamper-proof certificate verification system using blockchain technology. A digitally signed certificate is first issued by an authorized entity and then posted on the blockchain with a distinct cryptographic hash that acts as the digital fingerprint of the certificate. Relevant metadata, such as issuer and recipient details, issue date, and expiration, are stored on the blockchain. The project intends to improve certificate verification security and dependability by utilizing the decentralized and immutable characteristics of blockchain technology. This will help to reduce the dangers of fraud, manipulation, and unauthorized access that are common in centralized systems.

## Project Introduction:

Certificate verification and validation using blockchain is a procedure that leverages blockchain technology to check the authenticity and integrity of digital certificates securely. Traditional certificate verification methods often rely on centralized authorities, such as certificate authorities or educational institutions, which can be prone to fraud, tampering, or data breaches. Increased transparency, trust, and speed can be gained in certificate validation and verification by utilizing the decentralized and immutable characteristics of blockchains. Blockchain is a distributed ledger technology that eliminates the need for a central authority by enabling several parties to manage a shared and synchronized database. In the context of certificate verification, blockchain serves as a tamper-proof and transparent platform where certificates and related information can be securely stored and accessed.

Here's a general overview of how certificate verification and validation using blockchain works:

* + 1. Issuing Certificates: When a certificate is issued, such as an educational degree or a professional qualification, the relevant information is recorded on the blockchain. This information typically includes details about the certificate holder, the issuing authority, the date of issuance, and any necessary credentials.
    2. Generating a Certificate Hash: A cryptographic hash function is used to generate a unique digital fingerprint (hash) of the certificate data. This hash acts as a digital representation of the certificate and is stored on the blockchain.
    3. Recording on the Blockchain: The certificate hash, along with additional metadata, is recorded on the blockchain as a transaction. This transaction is added to a block and linked to the previous block, forming a chain of blocks (hence the term "blockchain"). This process ensures that the certificate data is securely stored and cannot be easily altered.
    4. Verification Process: When someone wants to verify a certificate, they can access the blockchain and retrieve the certificate hash. They can then compare this hash with the actual certificate to ensure its integrity. By comparing the hashes, any tampering or modification of the certificate can be easily identified. Additionally, the transparency of the blockchain allows anyone to independently verify the certificate without relying on a centralized authority.
    5. Accessibility and Efficiency: With blockchain-based certificate verification, the certificate holder has increased control and ownership over their credentials. They can

easily share their certificate hash with employers, educational institutions, or any other interested party, allowing for efficient and secure verification processes. This eliminates the need for time-consuming and potentially insecure manual verification methods.

* + 1. Smart Contracts (Optional): Smart contracts, programmable self-executing agreements, can be utilized in the block chain system to automate certain verification processes. For example, a smart contract can automatically validate a certificate if certain conditions are met, such as expiration dates or prerequisites.

By leveraging block chain technology, certificate verification and validation can offer enhanced security, transparency, and efficiency compared to traditional methods. It reduces the reliance on centralized authorities, mitigates the risk of fraud or tampering, and provides individuals and organizations with a reliable and decentralized system for verifying certificates.

# CHAPTER-2 LITERATURE SURVEY

## 2.1 Related Work:

1. **” An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends” by Zibin Zheng. (2017).**

An Overview of Blockchain Technology by Zibin Zheng offered comprehensive information on blockchain. It developed a number of technical phrases related to this technology, the most significant of which is the term "smart contract." The Blockchain creates a lengthy chain of nodes by storing the data's hash in the block before it. When data is tampered with, its hash changes and doesn't match the hash value saved in the previous block, alerting us to the change.

## Conclusion:

In conclusion, Zibin Zheng's paper "[1] An Overview of Blockchain Technology" effectively demystifies this intricate technology by introducing key terms and highlighting the critical concept of smart contracts. It emphasizes the inherent security of blockchain through its chain-like structure, where data tampering alters the hash and triggers immediate detection. This tamper-proof mechanism underpins the trust and transparency central to blockchain's potential for revolutionizing diverse fields. Zheng's paper thus provides a valuable foundation for further exploration and application of this disruptive technology.

## “Blockchain and Smart Contract for Digital Certificate,” by Jiin-Chiou. (2018)

The Software was created by Jin-chiou et al. to prevent certificate forgeries. The graduation certificate is to be forged because there is no anti-forge device in place. Thus, the Ethereum blockchain technology served as the foundation for the construction of the decentralized application. Create a hash value for the certificate and store it in the blockchain system after creating the digital certificate for the paper certificate. It required a different scanning app to scan the certificate, even when it was used to confirm the legitimacy of the document. The technology prevents document falsification and saves paper. However, a smartphone must be used to scan the QR code, and an internet connection is needed.

## Conclusion:

In conclusion, Jin-chiou et al.'s software solution represents a step forward in combating certificate forgery by leveraging blockchain technology. The system's effectiveness in preventing document forgery is notable, although the dependence on smartphone scanning and internet connectivity should be considered in the context of accessibility and widespread adoption. Future developments may focus on optimizing user accessibility while maintaining the security benefits of blockchain-based certificate verification systems.

1. **"Certificate Transparency Using Blockchain," by D.S.V.Madala.(2018)** The Hyper Ledger Fabric blockchain platform was utilized by Madala et al. [3]. In this system, Certificate Transparency (CT), a Google invention, requires domain owners' agreement before CAs can issue certificates. The goal is to stop SSL/TLS CAs from providing certificates for a domain without the domain owner's knowledge. However, there were fewer transactions and poor scalability.

## Conclusion:

In conclusion, while Madala et al.'s system introduces a robust security mechanism through the integration of Hyperledger Fabric and the CT technique, addressing scalability and transaction limitations is crucial for ensuring its feasibility and widespread adoption. Future developments and optimizations should focus on enhancing the system's performance to meet the demands of real-world scenarios without compromising the security principles established in the design.

1. **“Blockchain-Based Identity Verification Model”, by Gunit Malik. (2019)** "Blockchain-Based Identity Verification Model," by Gunit Malik [4]. Their system was composed of an issuing authority that created the document, a hashing algorithm that processed it, and a storage unit that held its value. They used asymmetric encryption to boost security because other systems used public hash keys.

## Conclusion:

In conclusion, Gunit Malik's model offers a promising framework for secure and efficient identity verification through the integration of blockchain and asymmetric encryption. However, further scrutiny and validation through real-world applications will be necessary to ascertain the model's effectiveness in diverse contexts. Future research efforts may focus on scalability, interoperability, and addressing potential challenges to ensure the practical viability and widespread adoption of this blockchain-based identity verification model.

## "Decentralized Digital Certificate Revocation System Based on Blockchain”, by Aisong Zhang. (2018)

Aisong Zhang and colleagues [5] developed a blockchain-based consortium framework. They employed a covert sharing plan. It has the ability to verify the digital certificate in order to safeguard user data and property. The CAs have worked together on the digital certificate revocation lists. When compared to the traditional approach, the CRL (Certificate Revocation List) is more trustworthy and dependable. The user simply needs to utilize the public key to decrypt the signature in order to validate the certificate. Additionally, the outcome will be contrasted with the message's original hash algorithm. Should the outcome remain constant, it would demonstrate that the digital certificate was unaltered. However, there is a delusion of security.

## Conclusion:

In conclusion, the system designed by Aisong Zhang et al. represents a noteworthy advancement in certificate validation through the utilization of consortium blockchain technology and a secret sharing scheme. The incorporation of digital certificate revocation lists (CRLs) shared among Certificate Authorities (CAs) enhances trust and reliability, surpassing traditional systems.

The system's approach to certificate verification, involving the decryption of signatures with public keys and subsequent comparison with the hash operation of the original message, provides a seemingly robust method for detecting tampering. However, it is crucial to acknowledge the potential existence of a false sense of security within this process. While the outlined steps may offer a layer of validation, it is imperative to consider the broader security landscape and potential vulnerabilities that might not be addressed by the current methodology.

## "Blockchain Technology in Education: The key to Lifelong Learning Passport" by T. Cobo et al. (2017).

The article is titled "Blockchain Technology in Education: The key to Lifelong Learning Passport" written by T. Cobo et al. (2017) examines the application of blockchain technology in the education sector, specifically focusing on the concept of a "Lifelong Learning Passport."

Here's an overview of the existing, proposed, and concluded aspects of the paper:

The authors discuss the limitations of traditional methods of verifying educational certificates and credentials, such as relying on centralized authorities and manual verification processes. They highlight the inefficiencies, potential for fraud, and lack of control for individuals over their educational records.

The paper proposes utilizing blockchain technology as a decentralized and secure solution for verifying and managing educational certificates. The concept of a Lifelong Learning Passport is introduced, which involves leveraging blockchain to create a digital identity that accumulates and securely stores an individual's educational achievements throughout their lifetime.

The authors suggest that by using blockchain, educational certificates can be stored as tamper- proof and transparent records, guaranteeing the information's integrity and veracity. The Lifelong Learning Passport would allow individuals to have direct control over their educational records, providing them with a portable and verifiable digital identity.

The proposed system would facilitate efficient and streamlined verification processes, as institutions or employers could directly access the blockchain to verify educational credentials. It would also promote interoperability by enabling the integration of certificates from different educational providers on the same blockchain.

## Conclusion:

The paper concludes by emphasizing the potential benefits of blockchain technology in the education sector. It highlights the decentralized nature of blockchain, which enhances security, trust, and efficiency in verifying educational certificates. The Lifelong Learning Passport concept, powered by blockchain, offers individuals greater control over their educational records and simplifies the verification process for institutions and employers.

The authors acknowledge the challenges associated with implementing blockchain technology in education, such as privacy, data protection, scalability, and the need for collaboration and standardization among educational institutions. However, they emphasize that the advantages of blockchain, including increased transparency, security, and efficiency, make it a promising solution for revolutionizing certificate verification and management in the education sector.

Overall, the paper advocates for the adoption of blockchain technology in education to create a Lifelong Learning Passport system, empowering individuals and transforming the way educational credentials are verified and shared.

## "Blockchain-Based Certificate Verification with Verifier-Privacy Preservation" by S. Kumari et al. (2018).

The research paper "Blockchain-Based Certificate Verification with Verifier-Privacy Preservation" by S. Kumari et al. explores the use of blockchain technology for certificate verification while ensuring the privacy of verifiers. The authors propose a novel approach that leverages block blockchain’s immutability and decentralization to enhance the security and trustworthiness of certificate verification processes.

The paper starts by discussing the limitations of traditional certificate verification systems, which often rely on centralized authorities. These systems are vulnerable to various attacks, such as certificate forging or revocation mishandling. The authors highlight the need for a more robust and tamper-proof solution to address these issues.

The main contribution of the paper is the introduction of a blockchain-based certificate verification system with verifier-privacy preservation. The authors propose the use of a public blockchain, where certificates are stored in a decentralized and transparent manner. The verification process involves multiple verifiers who maintain their privacy while validating the authenticity of certificates.

The proposed system utilizes cryptographic techniques, such as digital signatures and hash functions, to ensure the integrity and confidentiality of the certificates. Smart contracts are employed to automate the verification process, therefore doing away with the requirement for centralized authorities. The authors also present a detailed architecture for the proposed system and outline the steps involved in certificate verification.

## Conclusion:

The paper concludes that the proposed blockchain-based certificate verification system provides several advantages over traditional approaches. By leveraging blockchain’s inherent properties, such as immutability and decentralization, the system offers enhanced security, transparency, and trust in certificate verification processes. The use of smart contracts

eliminates the need for intermediaries, reducing costs and potential vulnerabilities. Moreover, the system ensures the privacy of verifiers by only revealing the necessary information during the verification process.

The authors acknowledge some challenges and limitations of their proposed system, such as scalability and reliance on public blockchains. They suggest further research to address these issues and explore the applicability of the proposed approach in real-world scenarios. Overall, the paper highlights the potential of blockchain technology in improving the efficiency and security of certificate verification systems while preserving the privacy of verifiers.

## "Blockchain-Based Certificate Verification System for Internet of Things" by V. Vignesh et al. (2019).

The existing system discussed in the paper focuses on the challenges faced in verifying certificates in the context of the Internet of Things (IoT). Traditional certificate verification systems rely on centralized authorities, such as Certificate Authorities (CAs), which can be prone to various security vulnerabilities and single points of failure. These limitations make traditional systems less suitable for the decentralized and dynamic nature of IoT environments.

The paper proposes a blockchain-based certificate verification system for IoT, which leverages distributed ledger technology to address the limitations of the existing systems. The proposed system aims to provide a secure, transparent, and decentralized mechanism for certificate verification in IoT environments. It utilizes the immutability and consensus features of blockchain to ensure the integrity and authenticity of certificates.

The key components of the proposed system include:

1. Certificate Generation: Certificates are generated for IoT devices and stored on the blockchain, including relevant information such as device identity and public key.
2. Blockchain Network: A distributed network of nodes maintains the blockchain ledger, ensuring consensus and immutability of certificate data.
3. Certificate Verification: Verification of certificates is performed by querying the blockchain network, eliminating the need for centralized authorities.
4. Smart Contracts: Smart contracts are employed to automate the certificate verification

process, enabling self-executing and tamper-resistant transactions.

1. Trust Management: The system incorporates a trust management mechanism to assess the reputation and reliability of IoT devices based on their behavior and interactions within the network.

## Conclusion:

The paper concludes that a blockchain-based certificate verification system for IoT can provide enhanced security, privacy, and reliability compared to traditional approaches. By leveraging the inherent features of blockchain, such as decentralization, transparency, and immutability, the proposed system offers a robust solution for certificate verification in IoT environments. It reduces the reliance on centralized authorities, mitigates single points of failure, and ensures the integrity of certificate data. However, the authors acknowledge that further research and development are needed to address scalability, performance, and interoperability challenges associated with implementing such a system in large-scale IoT deployments.

## "Decentralized Certificate Transparency and Secure Certificate Revocation using Blockchain" by S. Hameed et al. (2020)

The research paper "Decentralized Certificate Transparency and Secure Certificate Revocation using Blockchain" by S. Hameed et al. explores the application of blockchain technology for decentralized certificate transparency and secure certificate revocation. The authors propose a novel approach that leverages blockchain’s transparency and immutability to enhance the security and reliability of certificate management systems.

The paper begins by discussing the limitations of traditional certificate management systems, particularly in the areas of certificate transparency and certificate revocation. The authors highlight the challenges faced by centralized certificate authorities in maintaining a trustworthy and transparent system. Existing approaches often suffer from issues such as centralized control, lack of transparency, and vulnerability to attacks.

The main contribution of the paper is the introduction of a decentralized certificate management system using blockchain technology. The authors propose the use of a public blockchain, where certificates are stored in a transparent and immutable manner. The system

employs smart contracts to automate the processes of certificate issuance, verification, and revocation.

The proposed system ensures transparency by allowing anyone to view the blockchain and verify the integrity of certificates. Certificate revocation is made more secure and efficient by leveraging the decentralized nature of the blockchain. The authors provide a detailed architecture for the proposed system, explaining the roles and interactions of the different entities involved

## Conclusion:

The paper concludes that the proposed decentralized certificate management system using blockchain offers several advantages over traditional approaches. By leveraging blockchain’s transparency and immutability, the system provides a trustworthy and tamper-proof repository for certificates. The decentralized nature of the system eliminates single points of failure and reduces the reliance on centralized certificate authorities.

The authors highlight that the proposed system addresses the limitations of existing approaches by providing transparency, security, and efficiency in certificate management. However, they acknowledge some challenges, such as scalability and the need for consensus mechanisms in public blockchains. The authors suggest further research to address these challenges and to evaluate the proposed approach in real-world scenarios.

Overall, the paper emphasizes the potential of blockchain technology in revolutionizing certificate management systems, offering enhanced security, transparency, and reliability. The proposed system provides a decentralized and secure platform for certificate transparency and revocation, addressing the limitations of traditional centralized approaches.

## "Blockchain-Based Certification Systems: A Systematic Literature Review" by A. Ali et al. (2021).

The existing system discussed in the paper focuses on examining the use of blockchain technology in certification systems across various domains. Traditional certification systems often rely on centralized authorities and manual processes, which can lead to issues such as fraud, data manipulation, and inefficiencies. The authors identify the limitations of traditional systems and highlight the need for more secure and reliable certification mechanisms.

The paper presents a systematic literature review of blockchain-based certification systems.

The review aims to identify the different approaches, architectures, and applications of blockchain technology in certification systems. The proposed system does not introduce a specific new system but provides an overview of existing research and developments in this field.

Decentralized Issuance and Verification: Blockchain-based certification systems allow for decentralized issuance and verification of certificates. This eliminates the need for central authorities and enables individuals or organizations to issue and verify certificates directly.

Immutability and Tamper-Resistance: The use of blockchain ensures the immutability of certificates, making it extremely difficult to tamper with or manipulate certification records. This enhances the trustworthiness and reliability of the certification process.

Transparency and Auditability: Blockchain-based certification systems provide transparency by allowing stakeholders to access and verify certification data in a transparent manner. Additionally, the decentralized nature of blockchain enables auditability, as all transactions and changes to the certification records are recorded on the distributed ledger.

Smart Contracts and Automation: Smart contracts are utilized in blockchain-based certification systems to automate various processes, such as certificate issuance, verification, and revocation. This streamlines the certification workflow and reduces the reliance on manual interventions.

Interoperability and Standardization: The interoperability of blockchain-based certification systems is a crucial aspect, enabling seamless integration with existing systems and cross- platform compatibility. Standardization efforts are necessary to ensure compatibility and consistency across different blockchain implementations.

## Conclusion:

The systematic literature review concludes that blockchain-based certification systems offer several advantages over traditional systems. The use of blockchain technology provides enhanced security, transparency, and tamper-resistance in the certification process. It enables decentralized issuance and verification, eliminating the need for intermediaries. However, the review also highlights the need for further research and development to address challenges such as scalability, privacy, interoperability, and governance in blockchain-based certification systems. Standardization efforts and real-world implementation studies are essential for the widespread adoption and practical implementation of blockchain in certification systems across various domains.

# CHAPTER-3

**RESEARCH GAPS OF EXISTING METHODS**

## EXISTING METHOD

The existing system of certificate verification and validation using blockchain employs a decentralized approach to enhance trust and security. Certificates are digitally signed by issuers and stored on the blockchain, ensuring their integrity and immutability. Verifiers can retrieve certificates from the blockchain and validate their authenticity by comparing cryptographic hashes. The distributed ledger provides a transparent and tamper-proof record of certificate transactions, eliminating the need for centralized authorities. Consensus mechanisms in the blockchain network validate and secure the certificate data, ensuring its validity. This blockchain-based system promotes trust, transparency, and efficiency in certificate verification, revolutionizing traditional approaches and mitigating risks of fraud or manipulation.

## Disadvantages:

1. **Certificate Creation:** The certificate issuer generates a digital certificate containing relevant information, such as the identity of the certificate holder, issuer, and any additional metadata. The certificate may also include a digital signature from the issuer to ensure its authenticity.
2. **Certificate Hashing**: A cryptographic hash function is applied to the certificate, generating a unique digital fingerprint called a hash. The hash serves as a compact representation of the certificate's data.
3. **Certificate Anchoring:** The certificate's hash is then anchored or stored on the blockchain. This process involves creating a transaction on the blockchain that includes the certificate's hash as part of its data.
4. **Consensus Mechanism**: The blockchain network reaches a consensus on the validity of the transaction and adds it to the blockchain. This consensus is typically achieved through mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), or other consensus algorithms employed by the blockchain network.
5. **Certificate Verification:** To verify a certificate, the verifier retrieves the certificate's hash from the blockchain. The verifier can independently compute the hash of the certificate they possess and compare it with the hash stored on the blockchain. If the hashes match, the certificate is considered valid and has not been tampered with.

# CHAPTER-4 PROPOSED METHODOLOGY

## PROPOSED METHOD

The proposed method of certificate verification and validation using blockchain introduces a decentralized and transparent approach. Certificates are generated and stored on the blockchain, leveraging its immutability and consensus mechanisms. Smart contracts are utilized to automate the verification process, enabling self-executing and tamper-resistant transactions. Verifiers can independently retrieve certificate data from the blockchain and validate their authenticity using cryptographic techniques. The distributed nature of the blockchain ensures transparency and auditability, reducing reliance on centralized authorities. This method enhances the security, trustworthiness, and efficiency of certificate verification, addressing the limitations of traditional systems and providing a robust solution for various domains, including supply chain, and identity management.

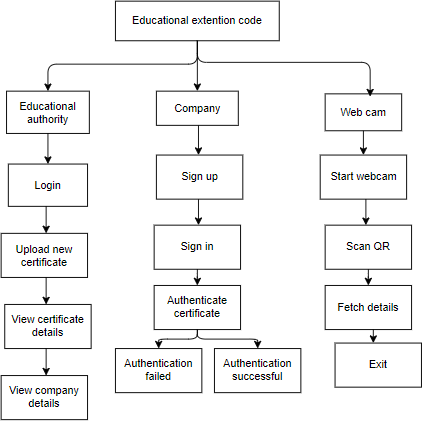
## Advantages:

1. **Enhanced Security**: Blockchain technology provides a high level of security by leveraging cryptographic techniques and consensus mechanisms. The immutability and tamper-resistant nature of the blockchain ensure the integrity and authenticity of certificates, reducing the risk of fraud or unauthorized modifications.
2. **Decentralization and Trust:** The decentralized nature of blockchain eliminates the need for a central authority, such as a certificate authority, making the verification process more transparent and resilient to single points of failure. This distributed trust model enhances trust among participants, as certificate verification can be performed by multiple nodes in the blockchain network.
3. **Transparency and Auditability:** The transparent nature of blockchain allows anyone to access and verify certificates stored on the blockchain. The entire transaction history, including the issuance and verification process, is recorded on the blockchain, providing an auditable and transparent trial for certificate validation.
4. **Efficiency and Cost Savings**: Blockchain-based certificate verification systems automate and streamline the verification process, reducing the need for manual interventions and paperwork. This improves efficiency, saves time, and reduces costs associated with traditional verification methods.
5. **Interoperability and Standardization:** Blockchain-based certificate verification systems

have the potential to promote interoperability and standardization across different industries and domains. The use of common blockchain protocols and standards can facilitate seamless integration and compatibility between various certification systems.

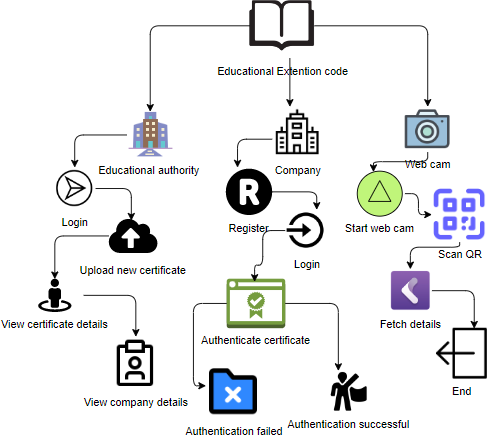
1. **Privacy and Data Ownership**: Blockchain technology allows for selective disclosure of certificate information, ensuring privacy while maintaining the ability to verify the validity of certificates. Users have control over their own certificate data and can choose when and how much information to disclose.

## Block Diagram:



**Figure 1**

* 1. **ARCHITECTURE:**



**Figure 2**

# CHAPTER-5 OBJECTIVES

Objectives for a project to store certificates in a decentralized way using blockchain:

* + - **Secure and efficient storage and verification of educational certificates**: To provide a secure and efficient way for individuals to store their educational certificates and for organizations to verify their authenticity.
    - **Decentralized storage:** To store certificates on a decentralized blockchain network, eliminating the need for a central authority and reducing the risk of data breaches or tampering.
    - **Digital signature and access control:** To allow individuals to sign their certificates digitally and control access to them by using multi-signature technology, requiring the consent of the individual and authorized organizations for access.
    - **Shareability:** To enable individuals to easily share their certificates with authorized organizations for verification purposes.
    - **Reduced workload for organizations:** To streamline the verification process for organizations by providing them with a secure and tamper-proof way to access and verify certificates.
    - **Increased transparency and trust:** To increase transparency and trust in the certificate verification process by providing a secure and auditable record of all certificate transactions.
    - **Reduced costs:** By eliminating the need for paper certificates and manual verification processes, the solution could potentially reduce costs for both individuals and organizations.
    - **Improved accessibility:** The solution could make it easier for individuals to access and share their certificates, regardless of their location.
    - **Enhanced security:** The use of blockchain technology could provide an additional layer of security for educational certificates, making them more resistant to fraud and forgery.

# CHAPTER-6

**SYSTEM DESIGN & IMPLEMENTATION**

## System Design:

**Input Design:**

The raw data that is used to create output in an information system is called input. The input devices, such as PC, MICR, OMR, etc., must be taken into account by the developers throughout the input design.

As a result, the system's output quality is determined by the quality of its intake. The following characteristics of well-designed input forms and screens are present:

* + - It should efficiently fulfill a certain goal, such as saving, recording, and retrieving information.
    - It guarantees accurate and correct completion.
    - It should be simple to fill out and easy to understand.
    - Its main goals should be simplicity, consistency, and user attention.
    - All of these are attained by applying an understanding of fundamental design concepts.

## Objectives for Input Design:

The input design's goals are −

* + - Creating input and data entry processes.
    - Reducing the amount of input and creating alternative data collection methods.
    - Designing source documents for data capture.
    - Developing user interface and data entry panels, among others.
    - Employing validation checks, and creating efficient input controls.

## Output Design:

The most crucial duty in every system is output design. Developers determine the necessary output types, prototype report layouts, and output controls during output design.

## Objectives of Output Design:

The objectives of output design are:

* + - To create output designs that fulfill requirements and prevent undesirable output from being produced.
    - To create an output design that satisfies the needs of the final user.
    - To provide the right amount of output.
    - To prepare the output in the proper format and send it to the correct individual.
    - To provide timely access to the output so that wise decisions can be made.

## UML DIAGRAMS

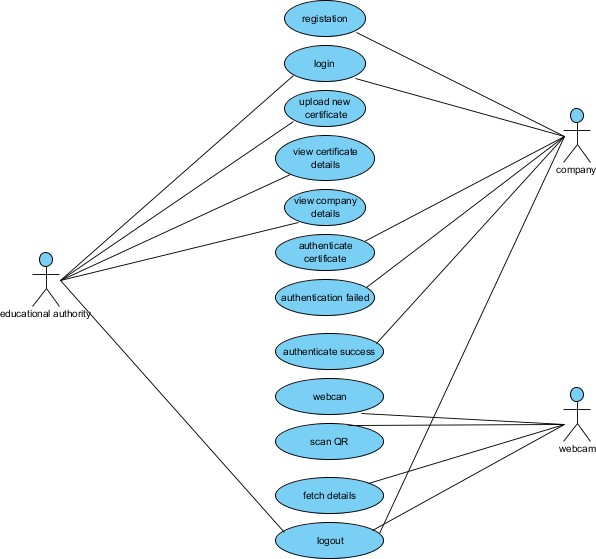
* + - Unified Modelling Language is known as UML. An industry-standard general-purpose modeling language used in object-oriented software engineering is called UML. The Object Management Group developed and oversees the standard.
    - The intention is for UML to spread as a standard language for modeling object- oriented software. The two main parts of UML as it exists now are a notation and a meta-model. In the future, UML may also include other processes or methods that are connected to it.
    - A common language for business modeling and other non-software systems, as well as for defining, visualizing, building, and documenting software system artifacts, is called Unified Modelling Language.
    - The UML is an assembly of top engineering techniques that have been successfully applied to the modeling of complicated and sizable systems.
    - Developing objects-oriented software and the software development process both heavily rely on UML. The UML primarily expresses software project design through graphical notations.

### GOALS:

The following are the main objectives of the UML design:

* + - * Give users access to an expressive, ready-to-use visual modeling language so they can create and share valuable models.
      * To expand the fundamental ideas, offer tools for specialization and extendibility.
      * Be unaffected by specific development processes or programming languages.
      * Offer a structured foundation for comprehending the modeling language.
      * Promote the market expansion for OO tools.
      * Encourage the use of higher-level development ideas like components, frameworks, partnerships, and patterns.
      * Combine the finest techniques.

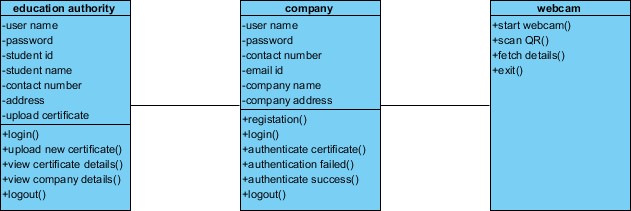
### USE CASE DIAGRAM

* + - * + According to the Unified Modeling Language (UML), a use case diagram is a particular kind of behavioral diagram that is produced from and defined by a use case study.
        + Its objective is to provide a graphical summary of the functionality that a system offers in terms of actors, use cases (representations of their goals), and any interdependencies among those use cases.
        + A use case diagram's primary goal is to display which actors receive which system functionalities. It is possible to illustrate the roles of the system's actors.

**Figure 3**

### CLASS DIAGRAM

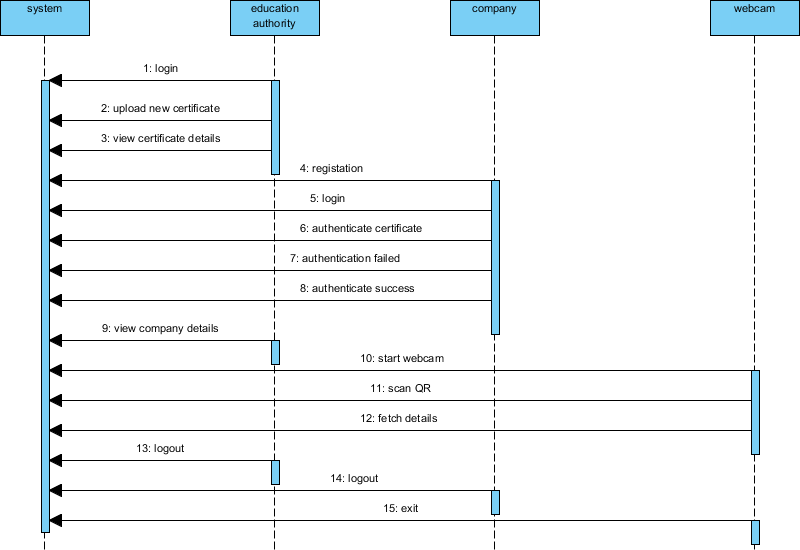
* + - A class diagram, in software engineering parlance, is a kind of static structural diagram in the Unified Modeling Language (UML) that illustrates a system's classes, attributes, operations (or methods), and relationships between the classes. It indicates which class has the data.



**Figure 4**

### SEQUENCE DIAGRAM

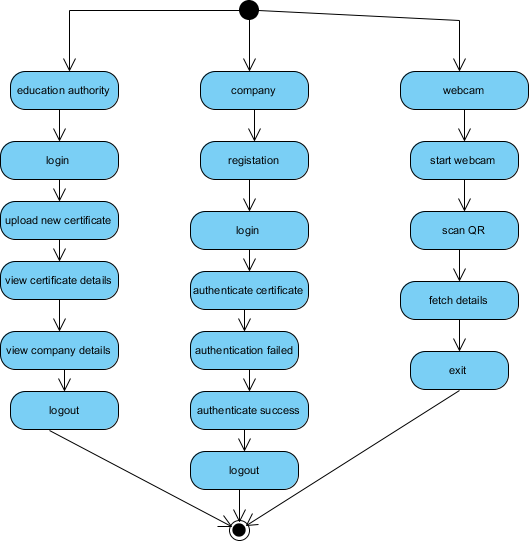
* + - One type of interaction diagram that illustrates how and in what order processes interact with one another is a sequence diagram in the Unified Modeling Language (UML).
    - It is a Message Sequence Chart construct. Event diagrams, event situations, and timing diagrams are other names for sequence diagrams.



**Figure 5**

### ACTIVITY DIAGRAM:

* + - Workflows of sequential activities and actions with support for choice, iteration, and concurrency are represented graphically using activity diagrams. Activity diagrams in the Unified Modelling Language can be used to explain the sequential business and operational workflows of system components. An activity diagram illustrates the total control flow.

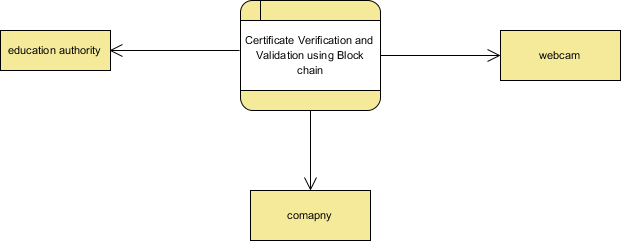


**Figure 6**

### DFD DIAGRAM:

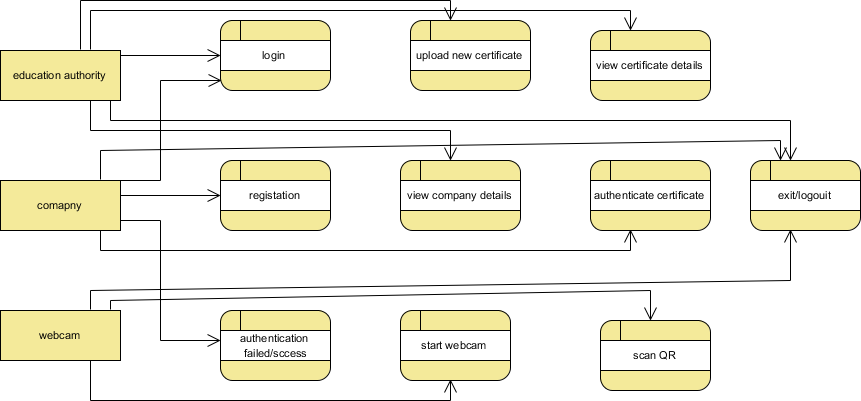
* The conventional method for visualizing the information flows within a system is a data flow diagram (DFD). A significant portion of the system requirements can be graphically represented by a clean, uncluttered DFD. It can be done manually, automatically, or both at once. It displays the flow of information into and out of the system, modifications made to the data, and locations of data storage. A DFD is used to illustrate the limits and scope of a system as a whole. It can serve as a communication tool between a systems analyst and any participant in the system, which serves as the foundation for system redesign.

### Level 0:



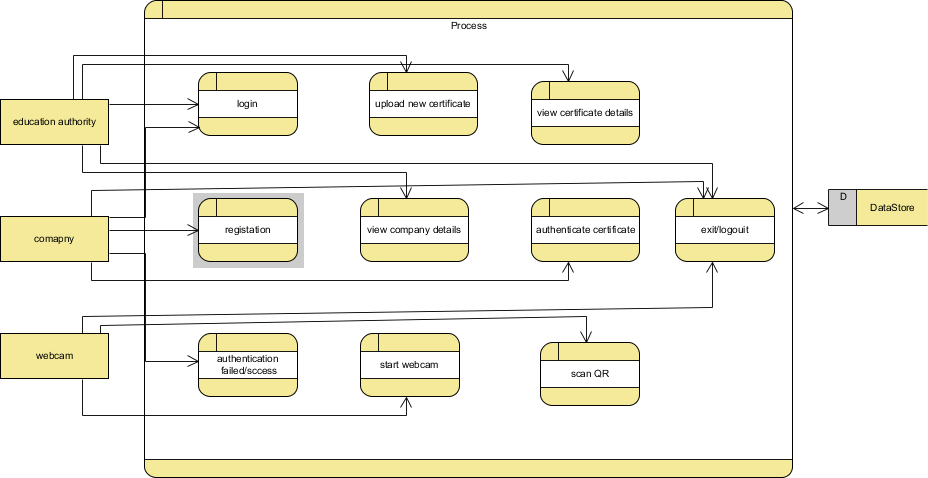
**Figure 7**

**Level 1:**



**Figure 8**

**Level 2:**



**Figure 9**

## IMPLEMENTATION

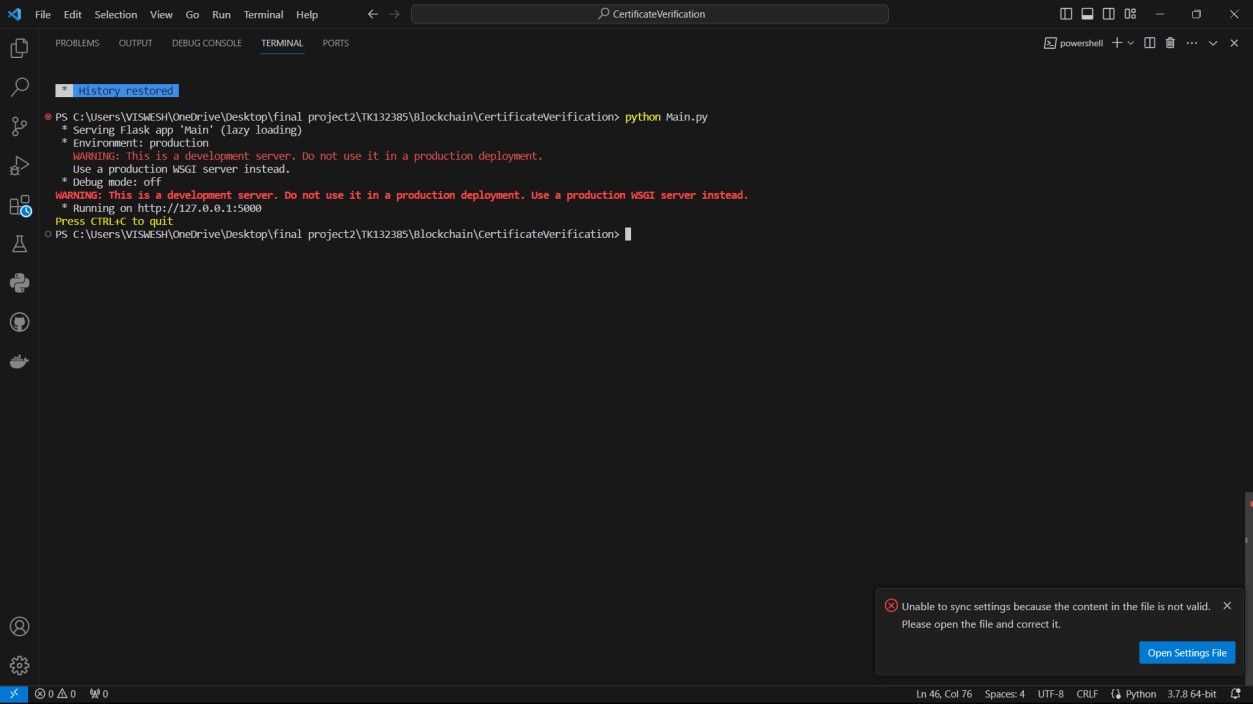
* 1. **MODULES:**

1. **Admin:** Admin is an education authority who login to the system using username and password as ‘admin’ and ‘admin’. After login admin will upload student details and certificates and these details will be uploaded to Blockchain and Blockchain associate each certificate with a unique hash code called a digital signature. QRCODE will also be generated on Hash code and affix on student certificate and this QR CODE can be scanned from mobile to get details from Blockchain and If there is a QR CODE in the blockchain, the certificate validation process is successful.
2. **Company:** The company user can sign up and login to system and then scan and upload certificate and then application will generate digital signature and matched with those signatures stored in Blockchain and if the certificate is authentic, an identical signature is generated, and the authentication process is successful.
3. **Scanner Module:** This is a standalone module which will maintain by education institution and companies and using this module they can scan QRCODE to get details from Blockchain

## Results:

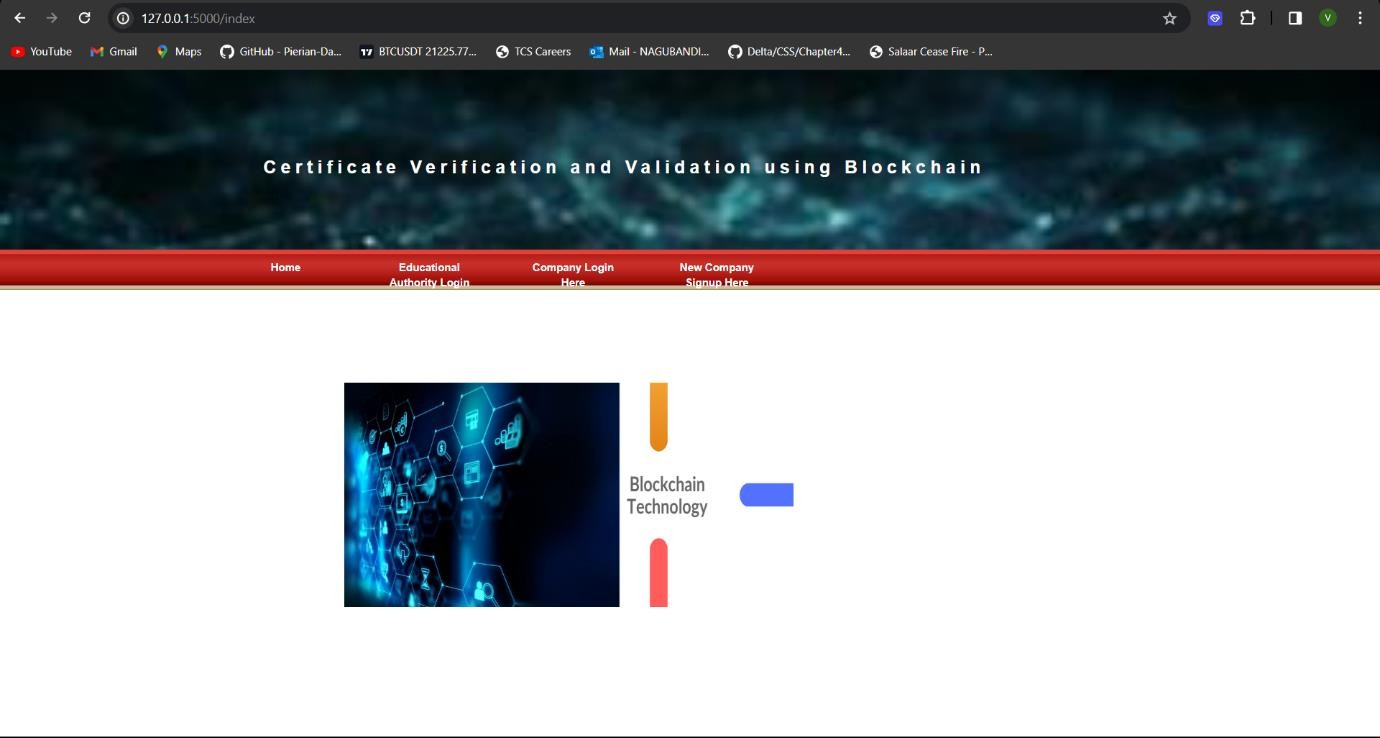
**Home page:**

To run project double click on ‘run.bat’ file to start python server and get below output



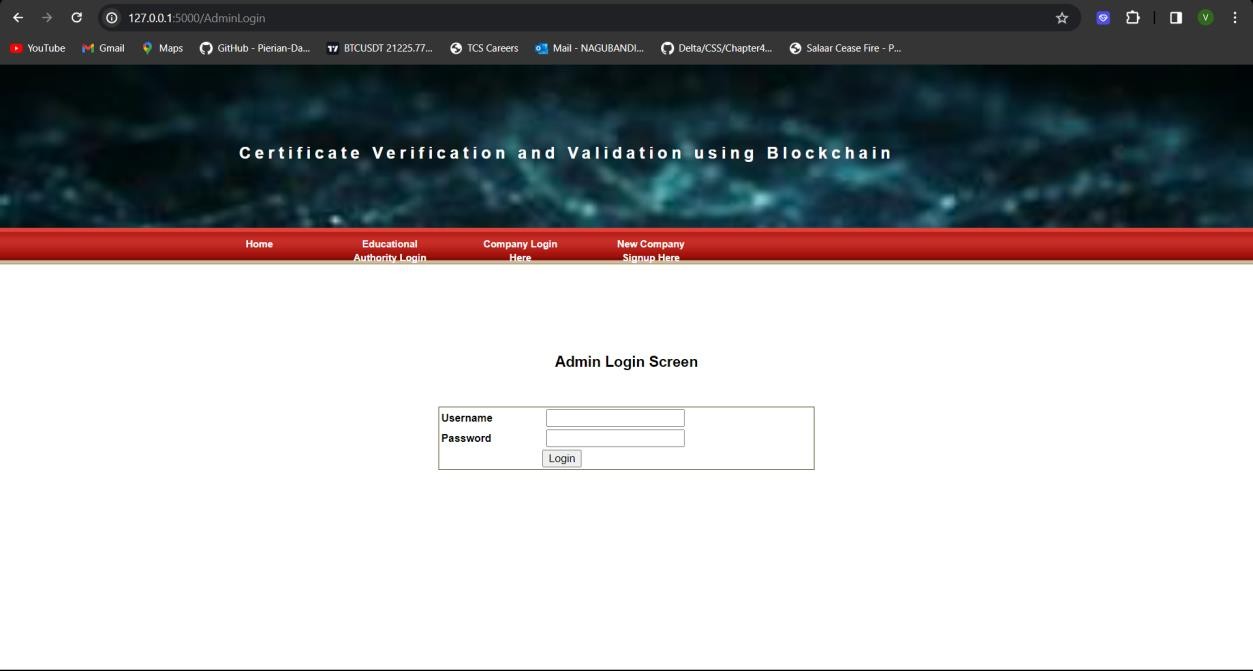
**Figure 10**

In above screen python FLASK server started and now open browser and enter URL as http://127.0.0.1:5000/index and press enter key to get below page



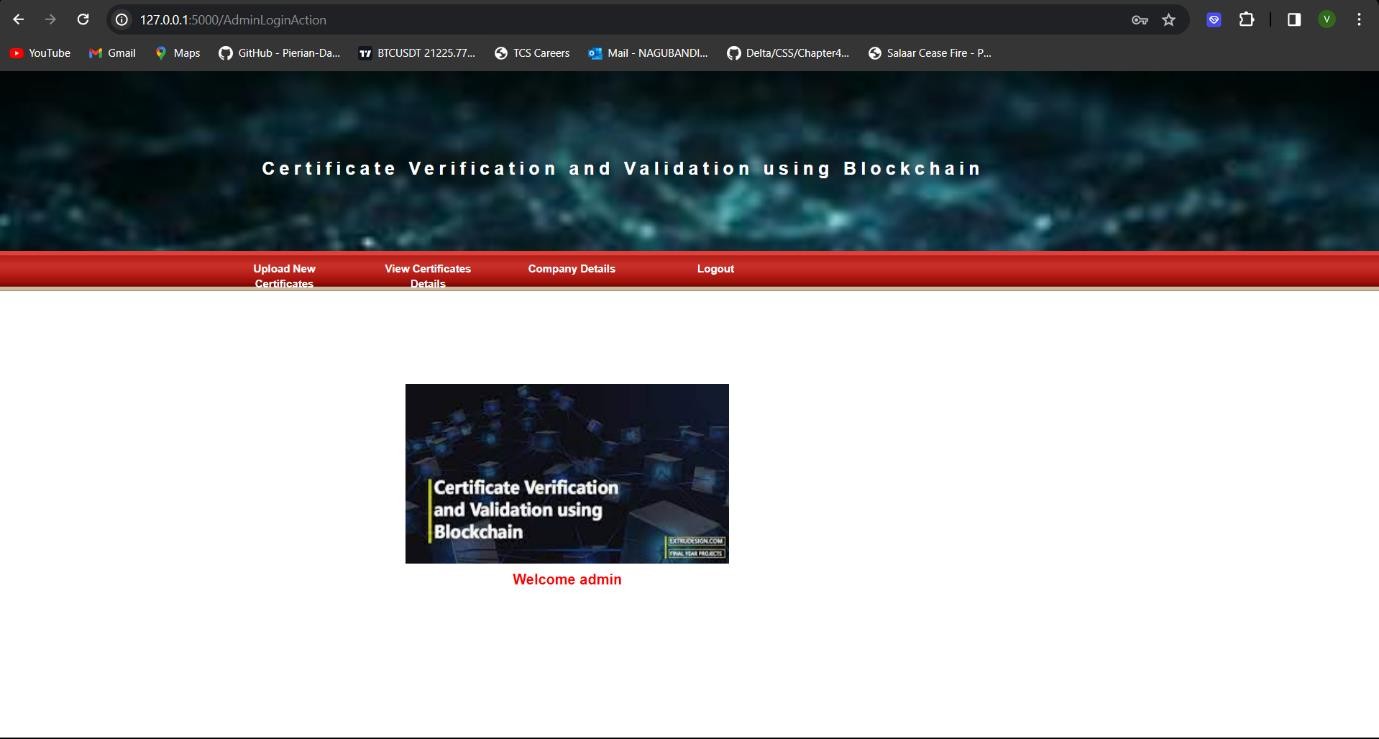
**Figure 11**

In above screen click on ‘Educational Authority Login’ link to get below login screen



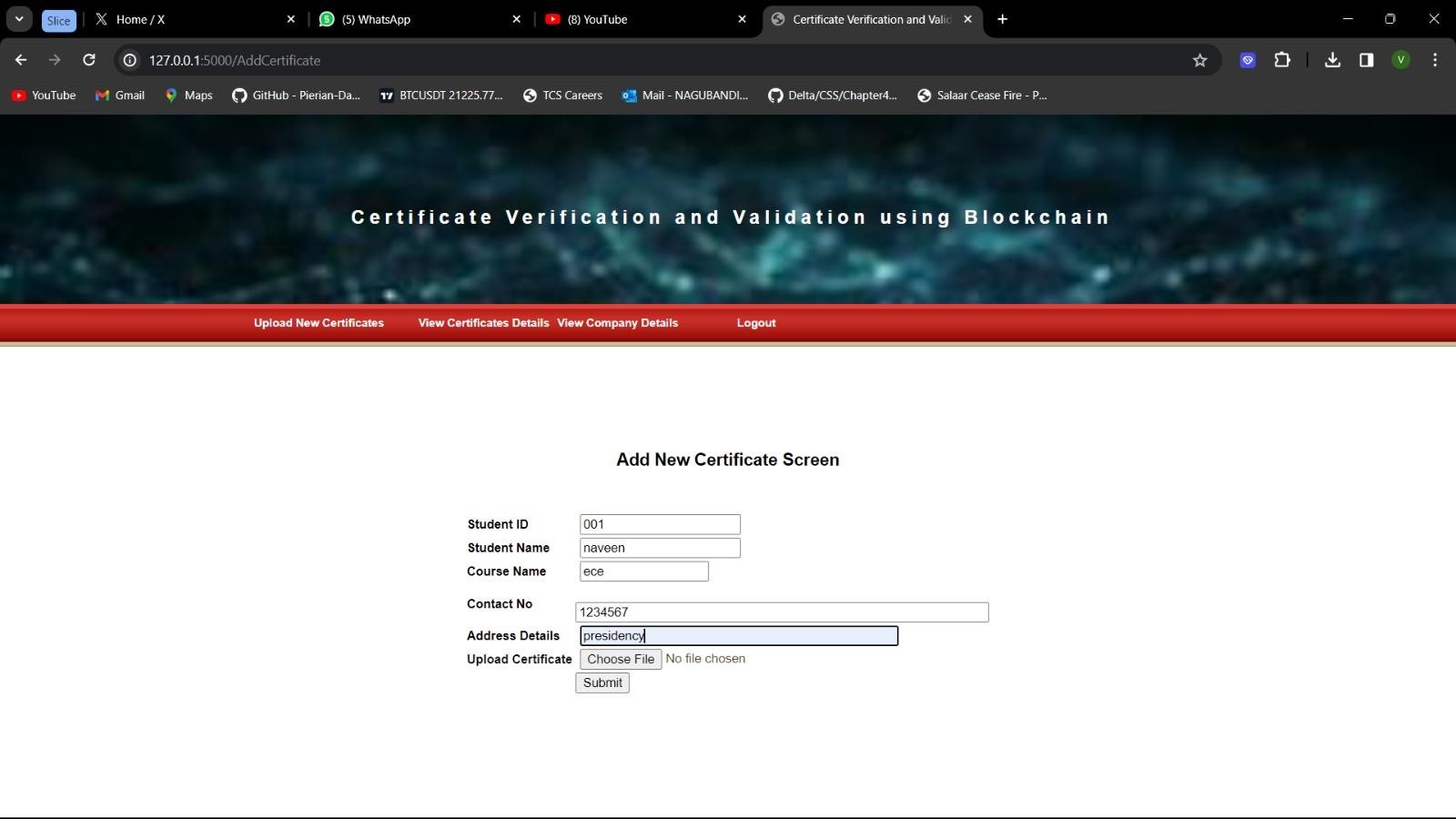
**Figure 12**

In above screen admin is login and after login will get below screen



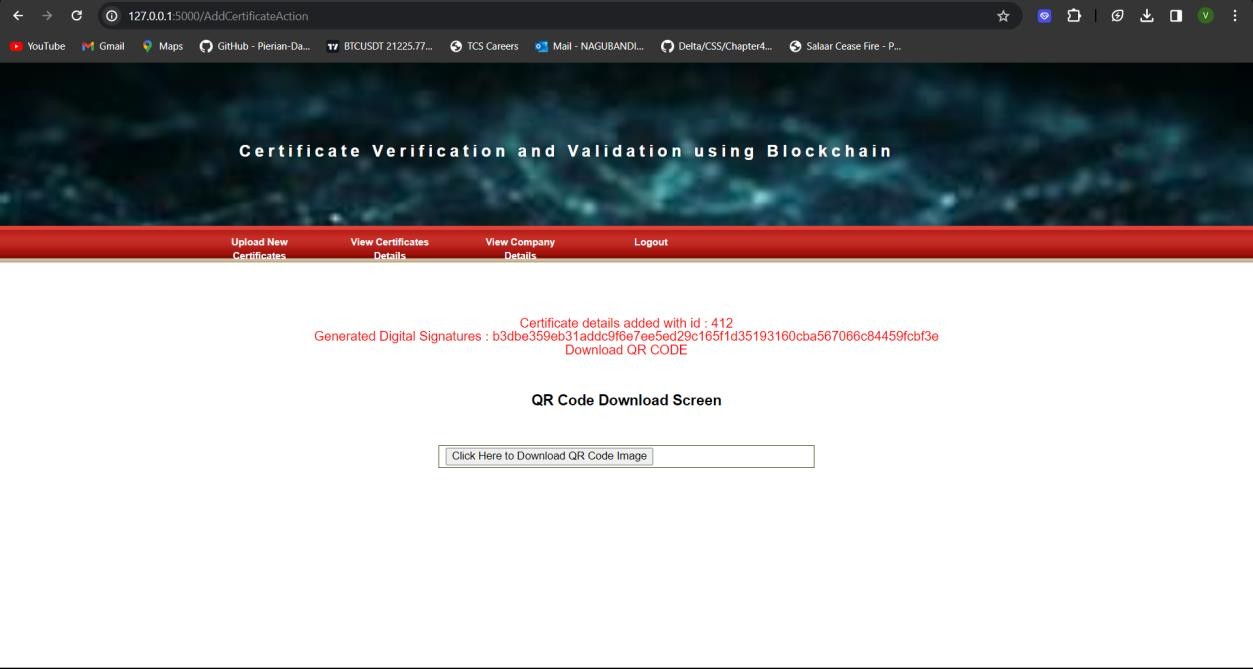
**Figure 13**

In above screen admin can click on ‘Upload New Certificates’ link to upload certificate



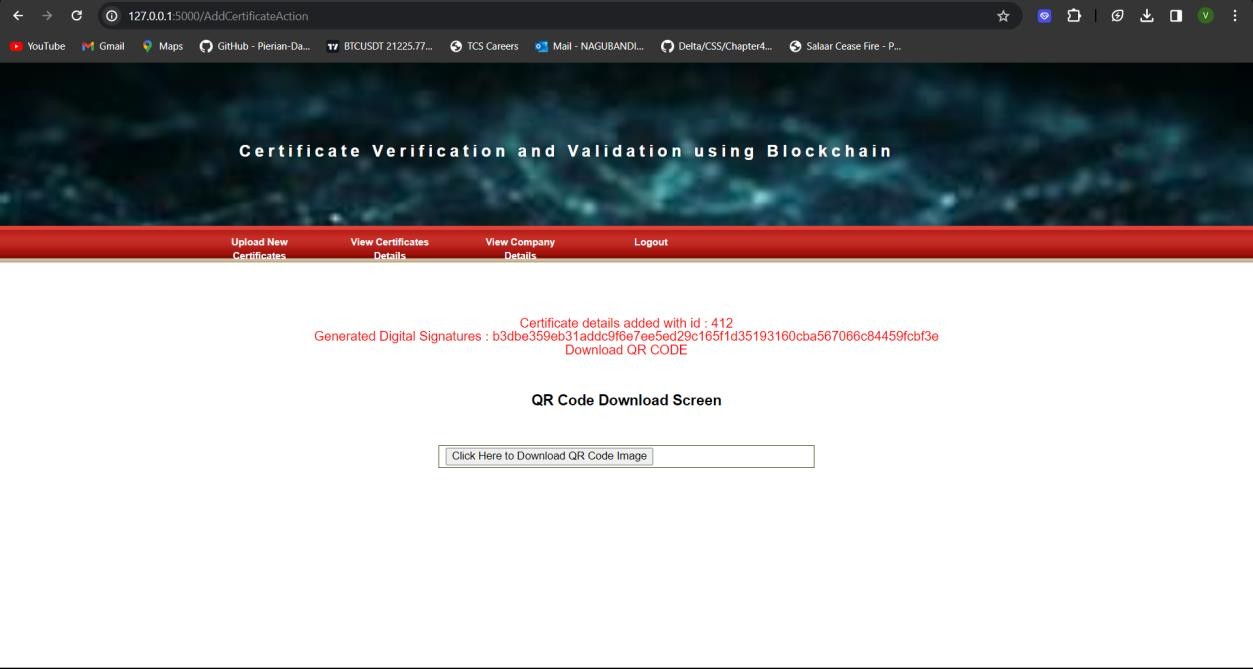
**Figure 14**

In the above screen admin is adding student details and then uploading the certificate and then pressing the ‘Submit’ button to get the below output



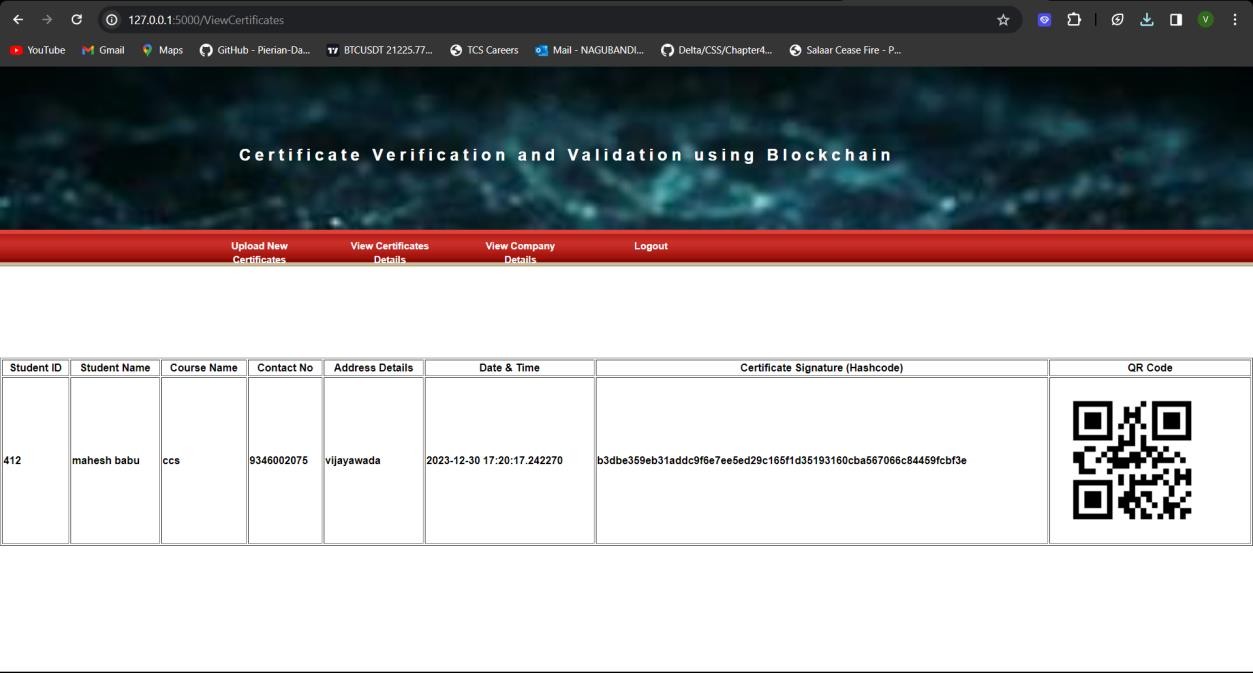
**Figure 15**

In the above screen student details were added and we can see a digital signature generated and stored in Blockchain for uploaded certificates now admin can click on the ‘Click Here to Download QR Code image’ button to download the QRcode and get the below output



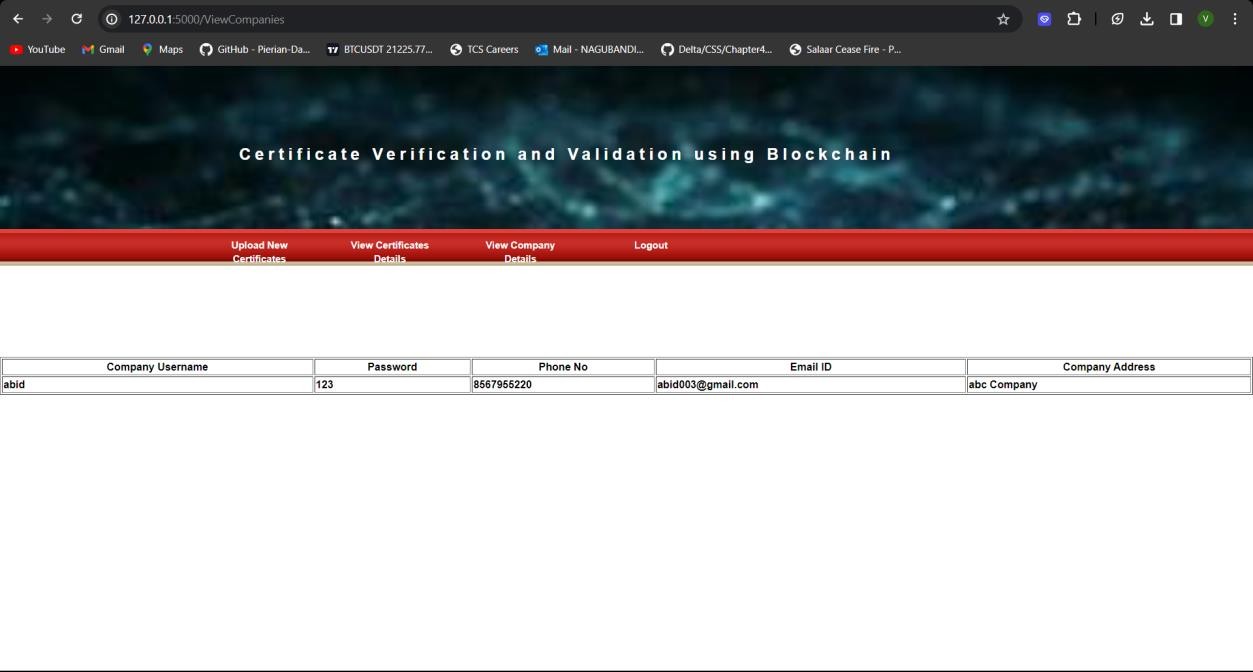
**Figure 16**

In above screen in browser status bar we can see QR code image downloaded and this image student can keep in his mobile. Now admin can click on ‘View Certificates Details’ to view all certificates stored in Blockchain



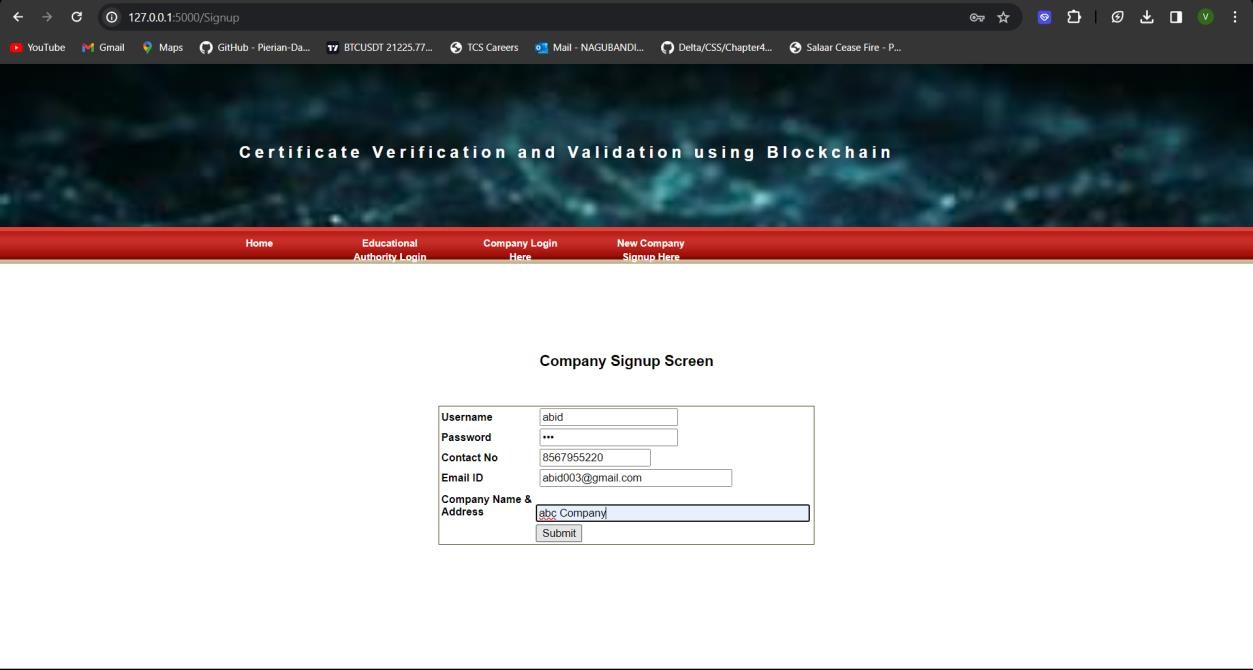
**Figure 17**

In above screen we can see different certificates of same or new student stored in Blockchain and we can see date and time of upload with digital signature and QR CODE image. Now admin can click on “View Companies Details’ to allow admin to view registered companies



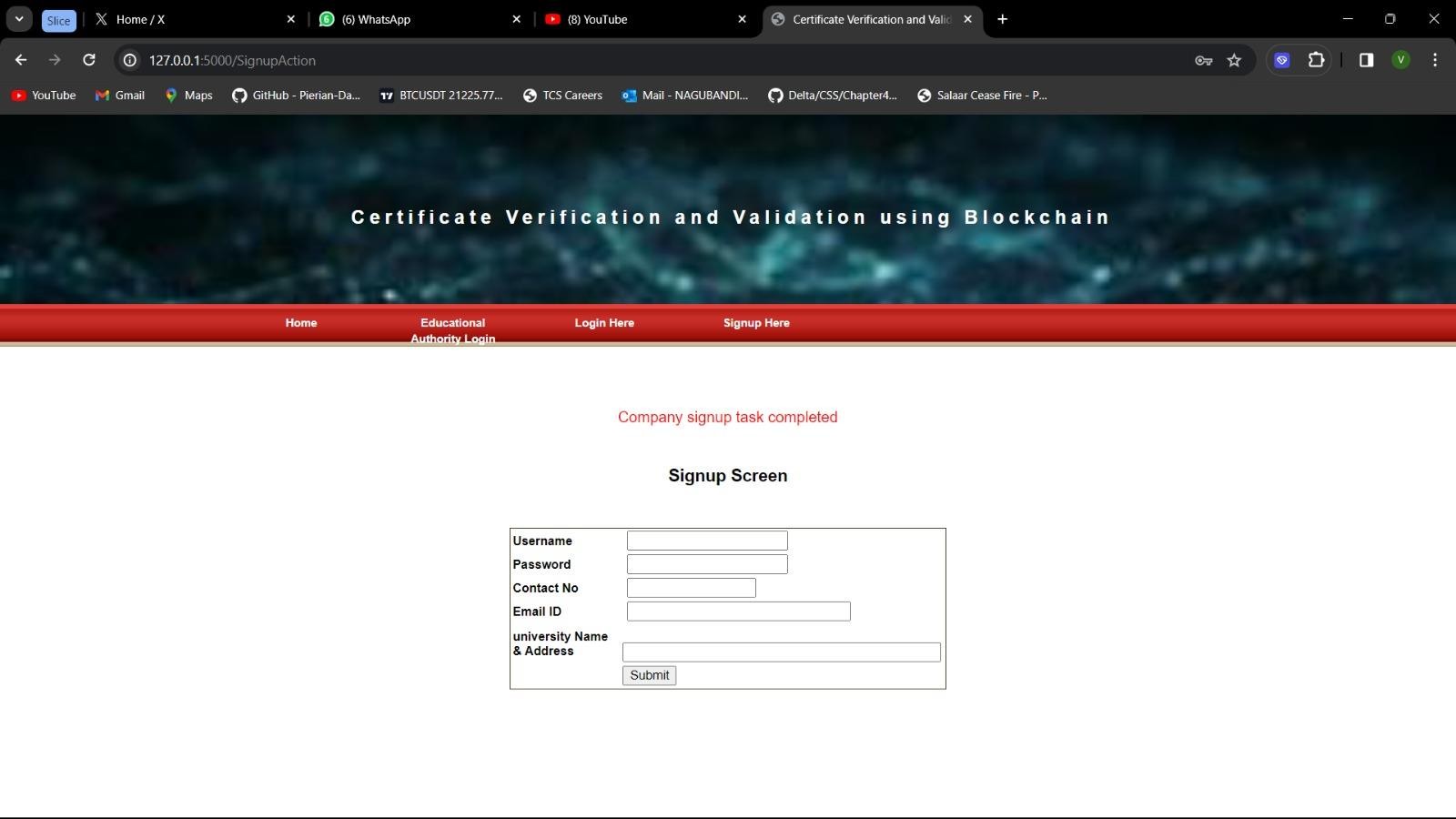
**Figure 18**

In above screen admin can view list of registered companies and now logout and signup new company to perform verification



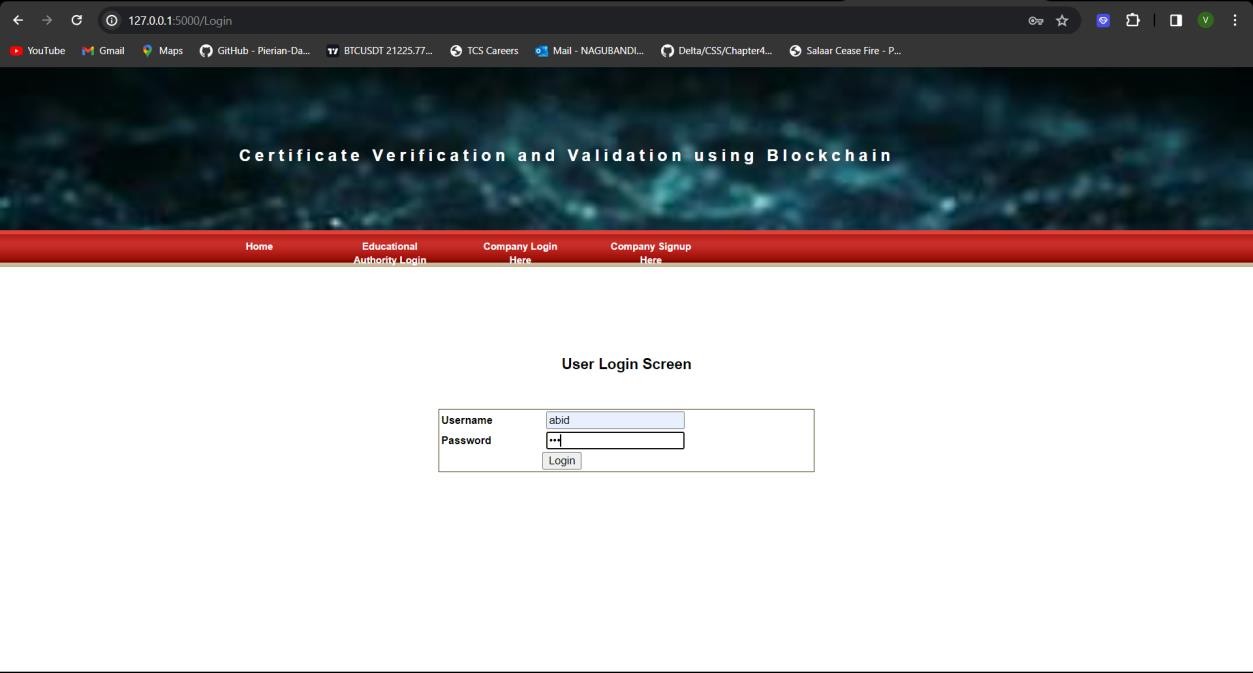
**Figure 19**

In above screen company is entering signup details and press button to store details in Blockchain and will get below output



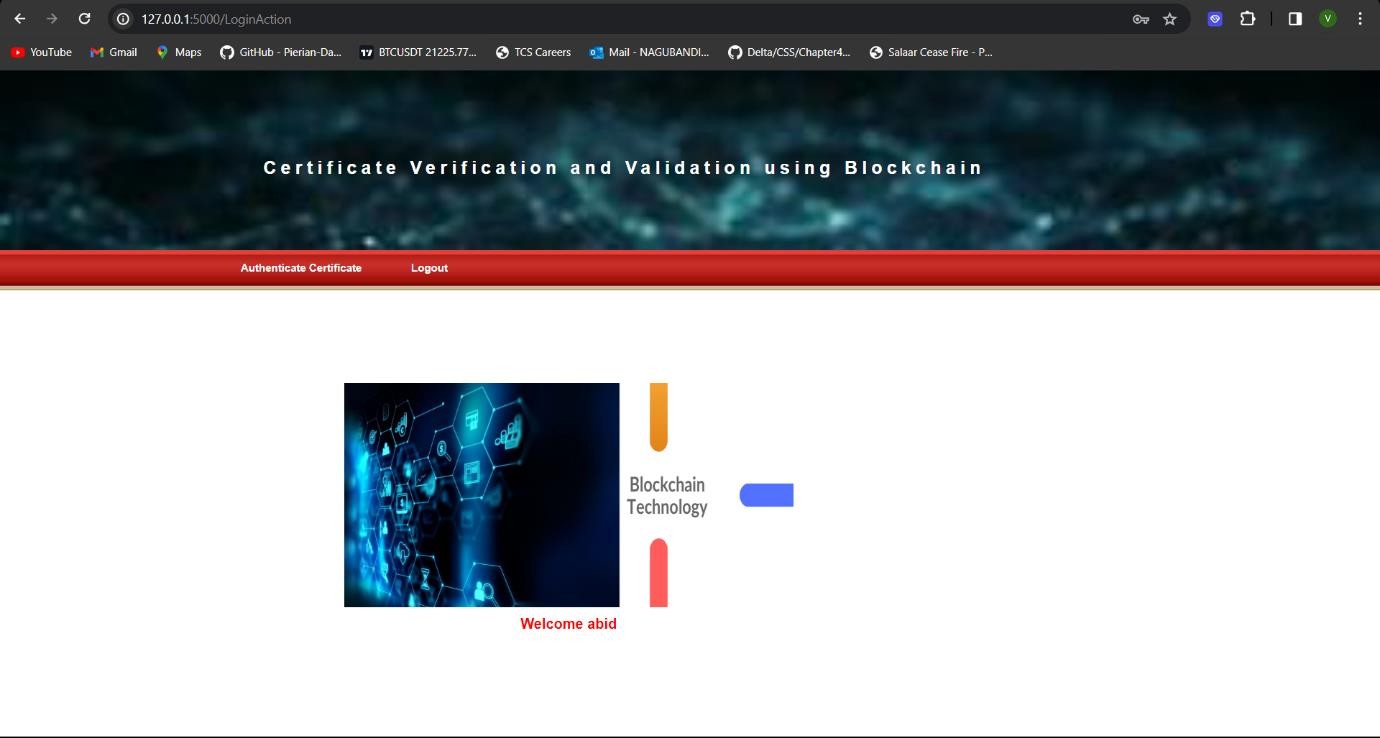
**Figure 20**

In above screen we can see company signup task completed and now click on ‘Company Login Here’ link to get below login screen



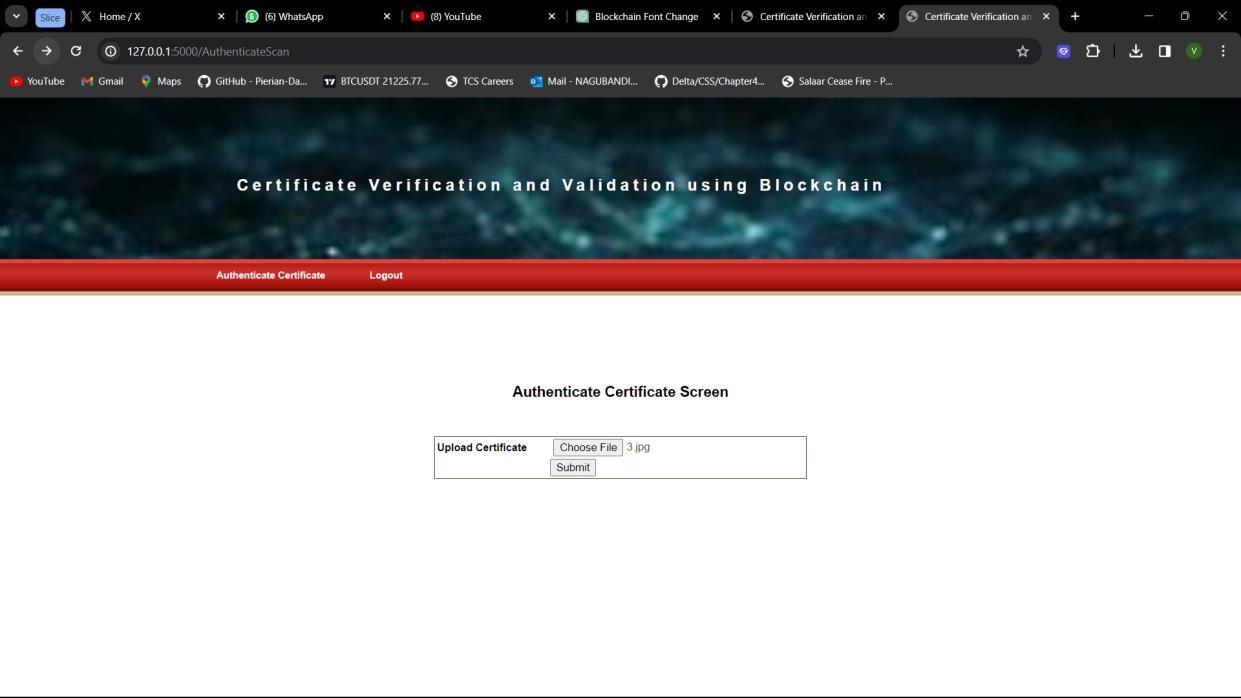
**Figure 21**

In above screen company is login and after login will get below screen



**Figure 22**

In above screen company can click on ‘Authenticate Certificate’ to upload certificate copy received from student and perform verification



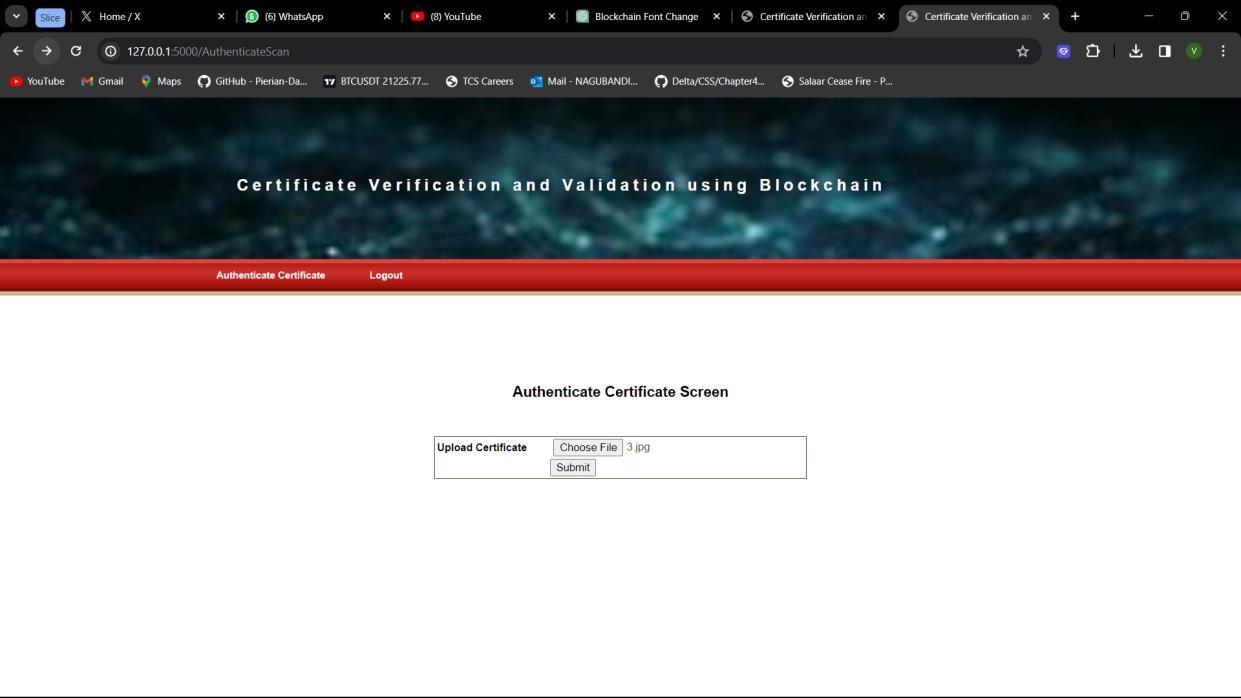
**Figure 23**

In above screen company can upload certificate and get below details if authenticated



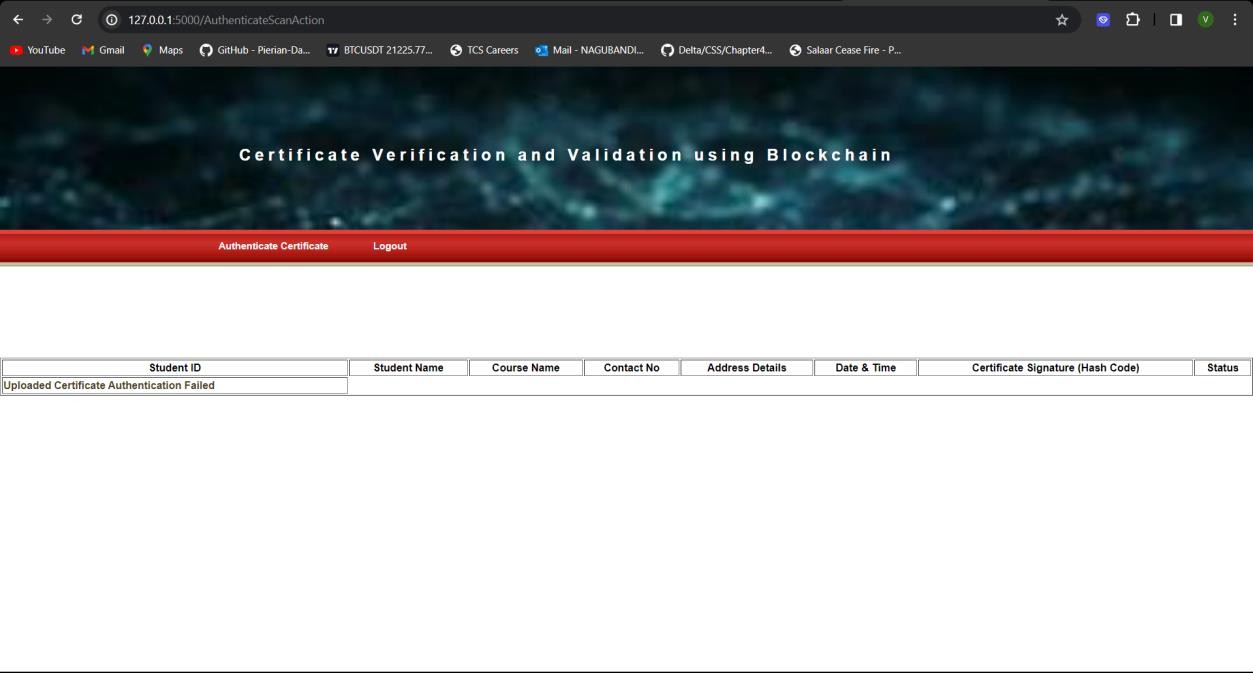
**Figure 24**

In above screen company can view all details of uploaded certificated and in last column we can see authentication successful and similarly they can upload and verify any certificate



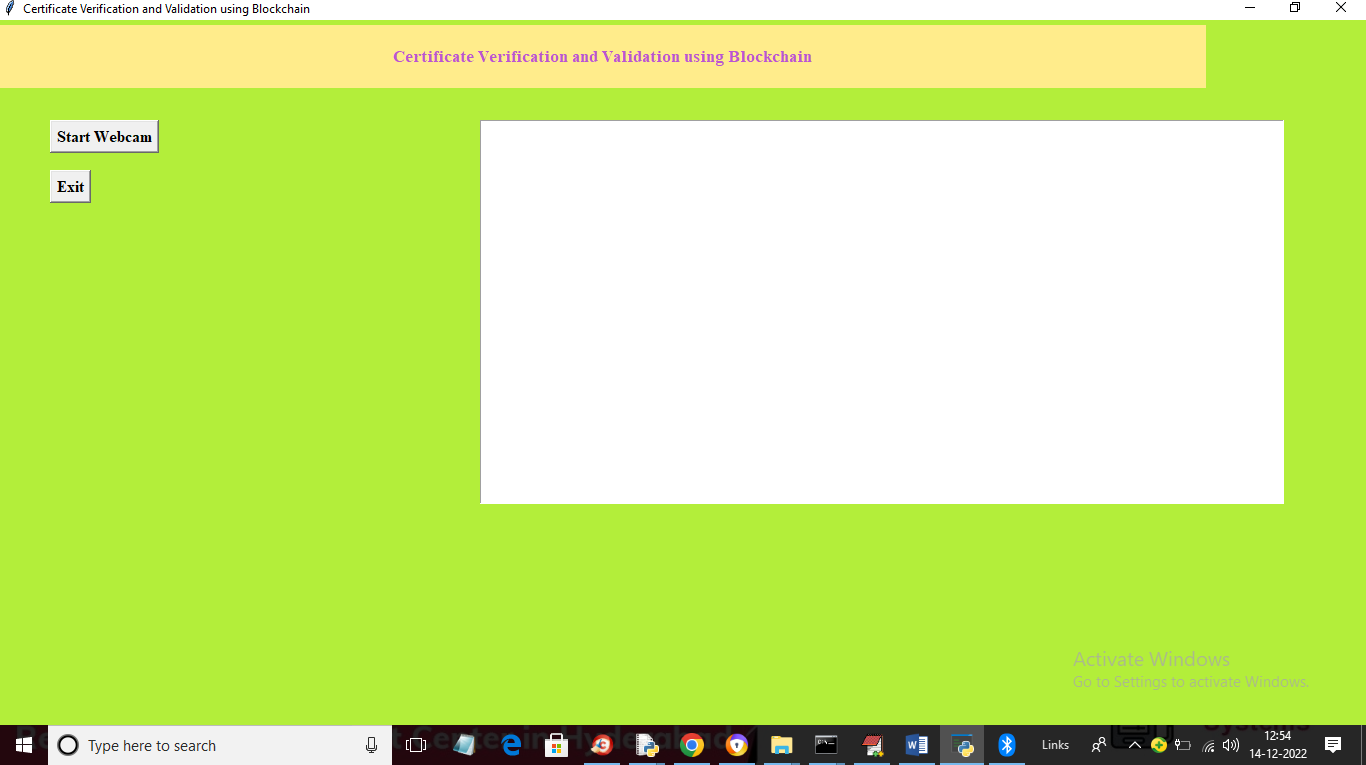
**Figure 25**

In above screen I am uploading another certificate and below is the output



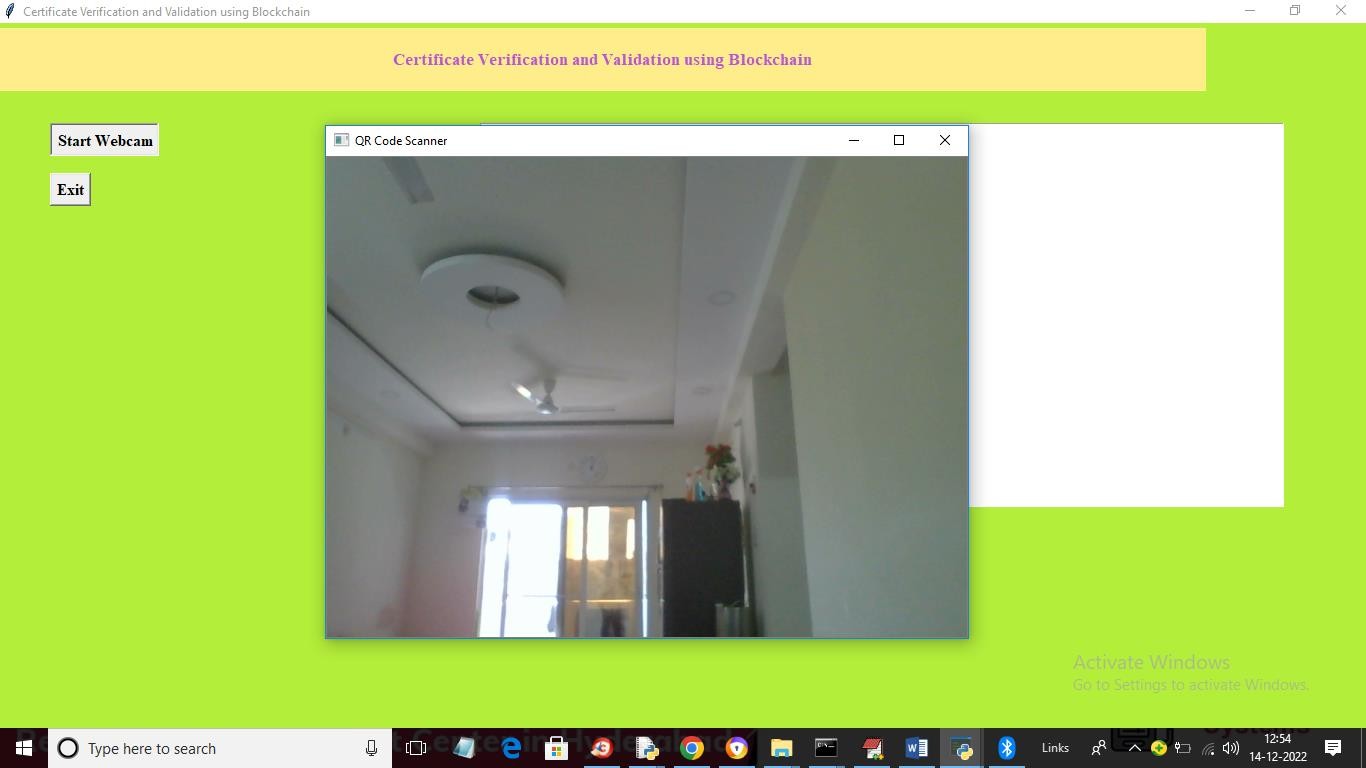
**Figure 26**

In above screen we can see Authentication failed for uploaded certificate.

Now company or educational institution can validate certificate by scanning QR code and to do that, just double click on ‘RunWebCam.bat’ file to get below output

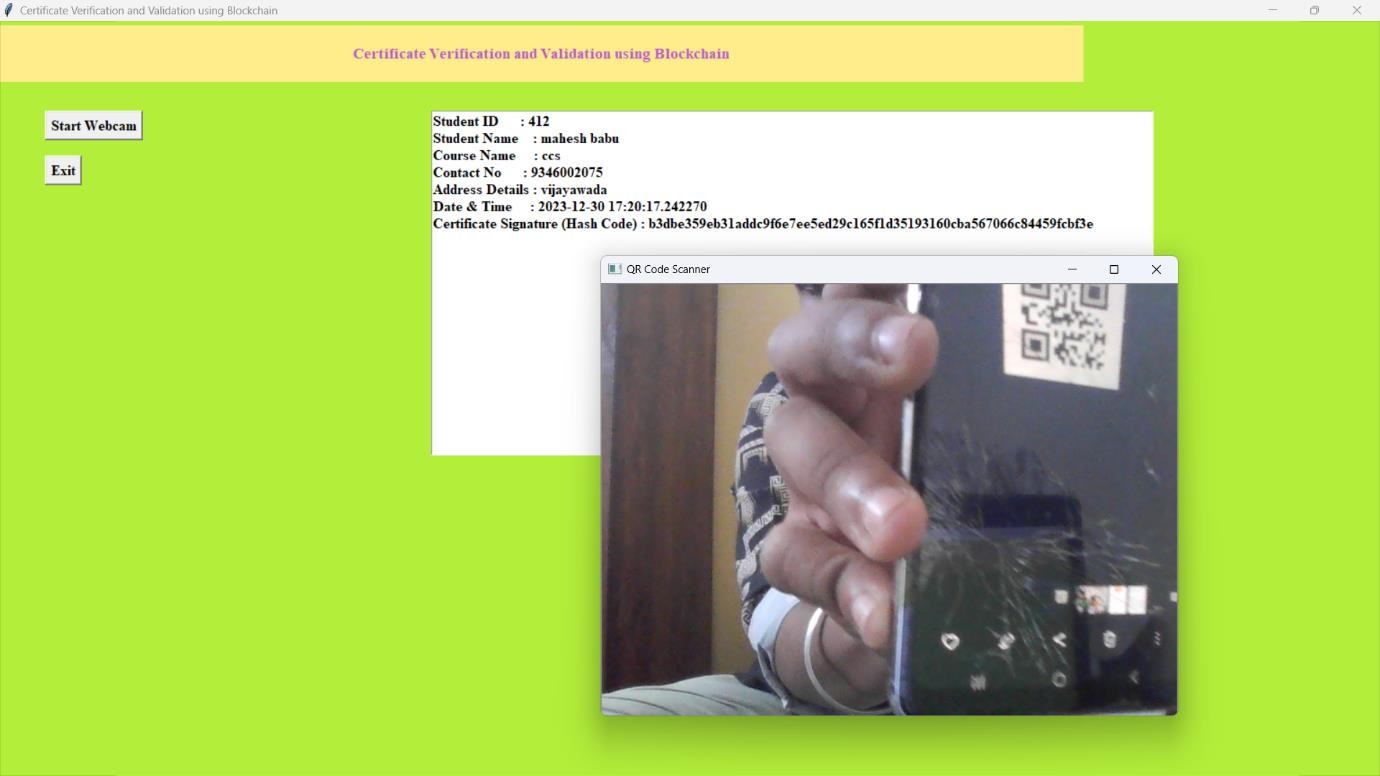
**Figure 27**

In above screen click on ‘Start Webcam’ button to start camera and get below output



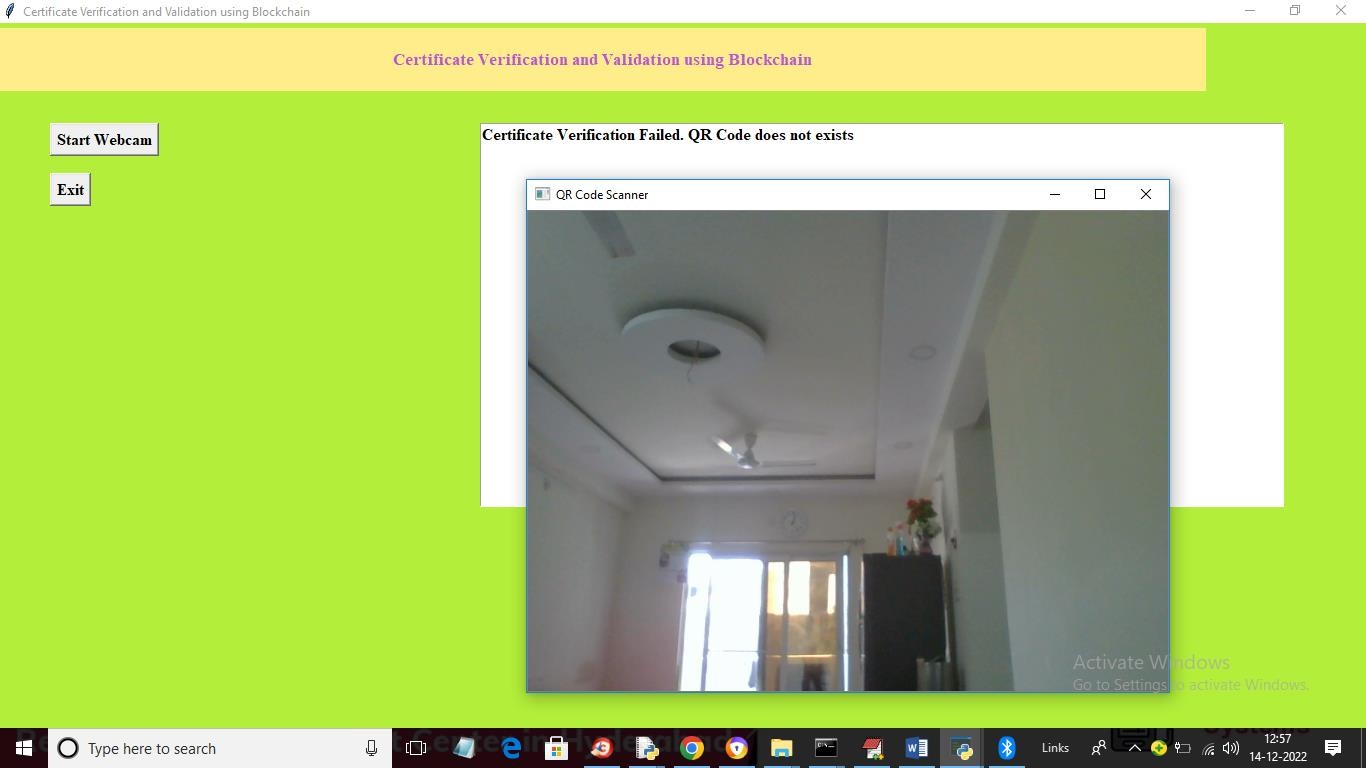
**Figure 28**

In above webcam from mobile they need to scan QRCODE like below screen



**Figure 29**

In above screen once we show QR code then all details for that QR code certificate will be retrieve from Blockchain and display in above TEXT area. Similarly if we scan wrong CODE then will get below output



**Figure 30**

In above screen we got message as Certificate validation failed as QR code does not exists.

### ABOUT SOLIDITY ETHEREUM ALGORITHM:

Solidity is not an algorithm but a high-level programming language specifically designed for developing smart contracts on blockchain platforms, with Ethereum being the most prominent. Ethereum itself operates on a consensus algorithm called Ethash.

### Purpose:

Smart contracts are self-executing contracts containing coded terms, and Solidity is made for developing such. It enables programmers to specify the guidelines and reasoning behind decentralized apps (DApps) that operate on the Ethereum network.

### Key Features:

Numerous data types, including as integers, booleans, texts, addresses, and more, are supported by Solidity.

Functions, events, modifiers, and libraries are among the elements that enable the creation of intricate and adaptable smart contracts.

After Solidity code has been compiled, the Ethereum Virtual Machine (EVM) runs the bytecode.

### Development Workflow:

The behavior of smart contracts is defined by developers using Solidity code. Bytecode is created by compiling the code.

A new instance of the smart contract is created when the bytecode is deployed to the Ethereum network.

Through transactions, users and other smart contracts can communicate with deployed contracts.

Ethereum Algorithm (Ethash):

### Consensus Mechanism:

Ethereum incorporates new blocks into the blockchain and verifies transactions using the Ethash proof-of-work (PoW) consensus mechanism.

### Mining Process:

Miners work through challenging math problems to identify a hash that meets requirements. The hash is broadcast to the network by the first miner to discover a legitimate one.

After the solution is confirmed by further nodes, the block is appended to the blockchain.**3. Gas and Transaction Fees:**

Gas is a unit that measures computational effort required to execute operations or deploy smart

contracts.

Users pay transaction fees in Ether, known as gas, to compensate miners for validating and executing transactions.

### Block Structure:

Each block contains a reference to the previous block, creating a secure and immutable chain. Transactions within a block are processed in a decentralized manner.

### Transition to Proof-of-Stake (PoS):

With Ethereum 2.0, Proof-of-Stake (PoS) will replace Proof-of-Whisk (PoW) in Ethereum. Enhancing scalability, energy efficiency, and security is the goal of this modification.

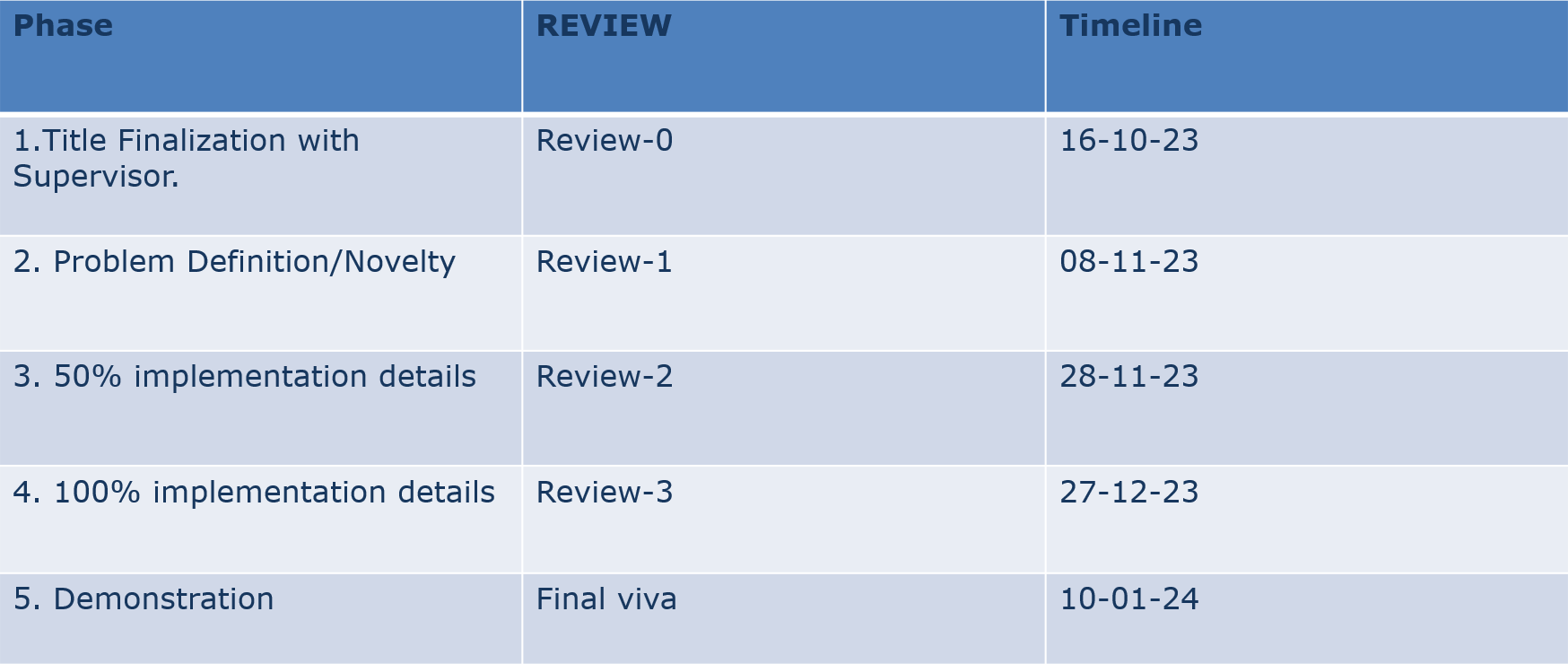
### Key Takeaway:

Solidity is a programming language for creating smart contracts, while Ethereum operates on the Ethash proof-of-work consensus algorithm. Together, they form the foundation for decentralized applications and transactions on the Ethereum blockchain. The upcoming transition to Ethereum 2.0 reflects efforts to address scalability challenges and enhance the overall efficiency of the Ethereum network.

# CHAPTER-7

**TIMELINE FOR EXECUTION OF PROJECT (GANTT CHART)**

## Timeline of Project:



**Table 1**

* 1. **GANTT CHART**



**Figure 31**

* 1. **Expected Outcomes:**

# CHAPTER-8 OUTCOMES

* + - **Increased security and authenticity:** Blockchain technology is highly secure and tamper-proof, making it ideal for storing important documents such as school/university/board certificates. Digital signatures ensure that the certificates are authentic and have not been tampered with.
    - **Reduced workload for organizations:** Institutions will no longer need to manually verify the authenticity of certificates, as this can be done automatically using blockchain technology. This will free up staff time and resources to focus on other tasks.
    - **Improved efficiency:** Students and graduates will be able to easily share their certificates with organizations or institutions with their consent, without having to worry about the security or authenticity of their documents. This can help to speed up the application process and reduce the risk of errors.
    - **Increased transparency:** Blockchain technology is transparent and public, which means that anyone can verify the authenticity of a certificate without having to contact the issuing institution. This can help to reduce fraud and increase trust in the system.
    - **Simplified sharing**: Sharing certificates with authorized organizations would be faster and easier, requiring only consent and no paperwork.
    - **Reduced costs**: Eliminating manual verification processes could lower operational costs for organizations.
    - **Reduced fraud:** The decentralized nature of the blockchain would make it difficult to forge or manipulate certificates.

However, the overall goal is to create a more secure, efficient, and user-friendly system for storing and verifying educational certificates, offering advantages for both individuals and organizations.

* 1. **Results**

# CHAPTER-9 RESULTS AND DISCUSSIONS

Our implementation of blockchain technology for certificate verification has not only elevated the security and integrity of digital certificates but has also revolutionized the validation process. The decentralized nature of blockchain not only ensures transparency but also fosters a collaborative and trustworthy ecosystem. The tamper-proof characteristics of the blockchain not only safeguard against unauthorized alterations but also establish a resilient and immutable platform. This fortification extends beyond individual certificates, creating a network effect that enhances the overall resilience and reliability of the entire verification infrastructure. As a result, our system not only instills confidence in the authenticity of individual credentials but also contributes to the broader paradigm shift towards more secure and transparent verification processes in diverse fields, reinforcing the resilience of digital transactions and record-keeping systems.

## Discussion

This blockchain-based approach goes beyond traditional methods, providing a paradigm shift in certificate verification marked by heightened security, transparency, and operational efficiency. Challenges encountered during implementation were diligently addressed, contributing to the creation of a robust system that proves scalable, capable of handling large volumes of certificates without compromising performance. The streamlined accessibility enhances the overall user experience, ensuring a seamless and user-friendly verification process.

Anticipating the future, our project envisions continuous improvement and development. We are committed to refining the system further, exploring avenues for enhanced functionality, and adapting to emerging technological trends. This commitment aligns with our broader goal of not just meeting current verification needs but also pioneering advancements that can potentially revolutionize the landscape. Looking forward, we foresee the potential for widespread adoption, envisioning a future where blockchain-based certificate verification becomes a standard, fostering increased trust and efficiency across various sectors.

# CHAPTER-10 CONCLUSION

In conclusion, the way certificates are validated might be completely changed by incorporating blockchain technology into the validation and verification procedures. This would guarantee increased security, openness, and confidence. The suggested approach offers a solid framework for putting into practice blockchain-based certificate verification systems while addressing the drawbacks of conventional techniques. Additionally, there is not much chance that students would misplace their certificates. The actual document will be saved in the InterPlanetary File System (IPFS), but the hash of the certificate is stored on the blockchain, reducing the amount of data that is tampered with by utilizing an additional hashing technique. By doing this, we can maintain the data and foster transparency.

Further research and development in this area can lead to widespread adoption and standardization of block chain technology for certificate verification across various industries and sectors.

# REFERENCES

* + 1. Zibin Zheng , Shaoan Xie, Hong-Ning Dai, Xiangping Chen , ” An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends”, IEEE 6th International Congress on Big Data, 2017.
    2. Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, “Blockchain and Smart Contract for Digital Certificate,” Proceedings of IEEE International Conference on Applied System Innovation 2018.
    3. D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, "Certificate Transparency Using Blockchain," 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, Singapore, 2018, pp. 71-80, doi: 10.1109/ICDMW.2018.00018.
    4. Gunit Malik, Kshitij Parasrampuria, Sai Prasanth Reddy, Dr. Seema Shah, “Blockchain Based Identity Verification Model”, International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019.
    5. Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain”, Journal of Physics: Conference Series, Volume 1069, 3rd Annual International Conference on Information System and Artificial Intelligence (ISAI2018) 22–24 June 2018, Suzhou.
    6. Ali, A., et al. (2021). Blockchain-Based Certification Systems: A Systematic Literature Review. Sensors, 21(4), 1233.
    7. Vignesh, V., et al. (2019). Blockchain-Based Certificate Verification System for Internet of Things. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-5). IEEE.
    8. Stukach, V., et al. (2019). Decentralized Blockchain-Based Certificate Validation for Learning Objects. In 2019 International Conference on Information Technology and Systems (ICITS) (pp. 1-6). IEEE.
    9. Alam, M. M., et al. (2019). A Blockchain-Based Secure Certificate Verification System. In 2019 4th International Conference on Networking, Systems and Security (NSysS) (pp. 1-6). IEEE.
    10. Bello, R. A., et al. (2019). Blockchain-Based Certification System for the Internet of Things. In 2019 IEEE 7th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 47-52). IEEE.

### Import Libraries:

* 1. **Import Flask modules:**

# APPENDIX-A PSUEDOCODE

* + - Flask: Primary module for creating the web application
    - Render\_template: For rendering HTML templates
    - Request: For handling incoming HTTP requests
    - Redirect: For redirecting users to different URLs
    - URL\_for: For generating URLs for routes within the application
    - Session: For managing user sessions
    - Send\_from\_directory: For serving static files (like images or certificates)

### Import blockchain modules:

* + - Web3: For interacting with the Ethereum blockchain
    - HTTPProvider: For connecting to an Ethereum node using HTTP

### Import other modules:

* + - Json: For working with JSON data
    - Hashlib: For generating hashes (e.g., for password security)
    - OS: For interacting with the operating system (e.g., accessing files)
    - Datetime: For working with dates and times
    - pyqrcode: For generating QR codes

### Create Flask Application:

* Create an instance of the Flask class and assign it to a variable (e.g., app = Flask(\_name\_))

### Set Secret Key:

* Set the app.secret\_key property to a secure string for session management

### Global Variables:

* Declare global variables to store user information and session data (e.g., uname, details, sid)

### Blockchain Interaction Functions:

* ReadDetails(contract\_type):
* Connect to a blockchain node using Web3
* Interact with the specified contract type
* Retrieve relevant data from the blockchain
* SaveDataBlockChain(currentData, contract\_type):
* Connect to a blockchain node using Web3
* Interact with the specified contract type
* Write the provided data to the blockchain

### Routes and Functionalities: Index:

* Render the index.html template (likely the homepage)
* Other routes (Login, AdminLogin, Signup, ViewCertificates, etc.):
* Handle specific user actions and interactions, often involving:
* Reading or writing data to the blockchain
* Rendering appropriate templates
* Redirecting users to different pages
* Processing form submissions

### Login and Signup:

* In /Login, validate user credentials against login records stored in the blockchain or a database.
* In /Signup, create a new user record on the blockchain or database and assign a unique ID.
* Consider implementing secure password hashing for improved security.
* Session Management:
* Upon successful login, generate a session ID and store it in a cookie or server-side session store.
* Use the session ID to track logged-in users and restrict access to unauthorized pages.
* Allow session logout functionality (e.g., /Logout) to clear the session ID and redirect to the login page.

### Certificate Management:

* Adding Certificates:
* In /AddCertificate, provide a form for users to enter certificate details like name,

issuing institution, date, etc.

* Upon form submission (/AddCertificateAction), validate the data and call the saveDataBlockChain function to write the certificate information to the blockchain.
* Viewing Certificates:
* In /ViewCertificates, query the blockchain based on user ID or search criteria and fetch relevant certificates.
* Render a list of certificates with details like name, issuer, and date on the ViewCertificates.html template.
* Downloading Certificates:
* In /DownloadAction, retrieve the complete certificate data from the blockchain for the chosen certificate.
* Generate a QR code containing the certificate details and allow users to download it as a PDF or image format.

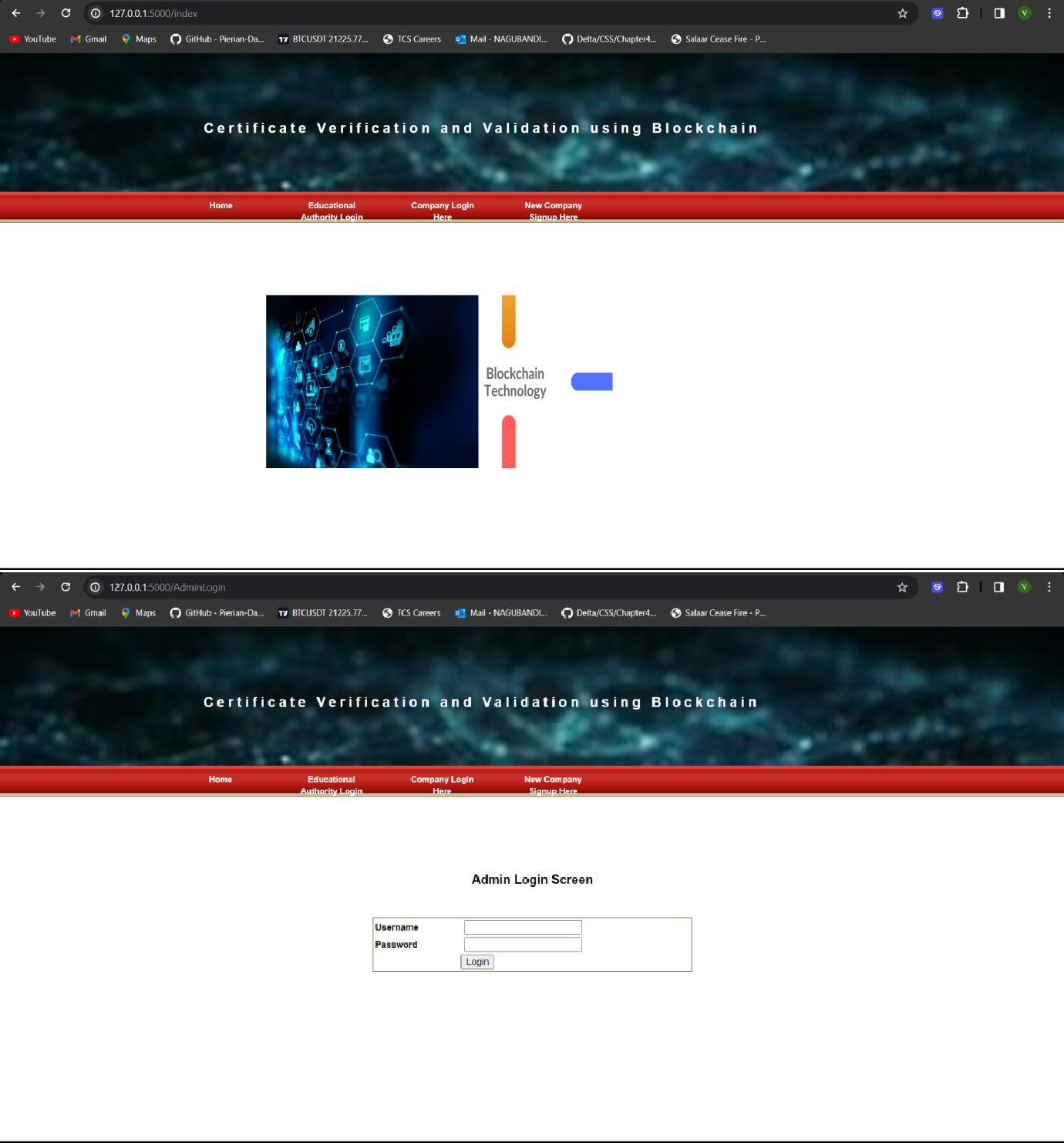
### QR Code Authentication:

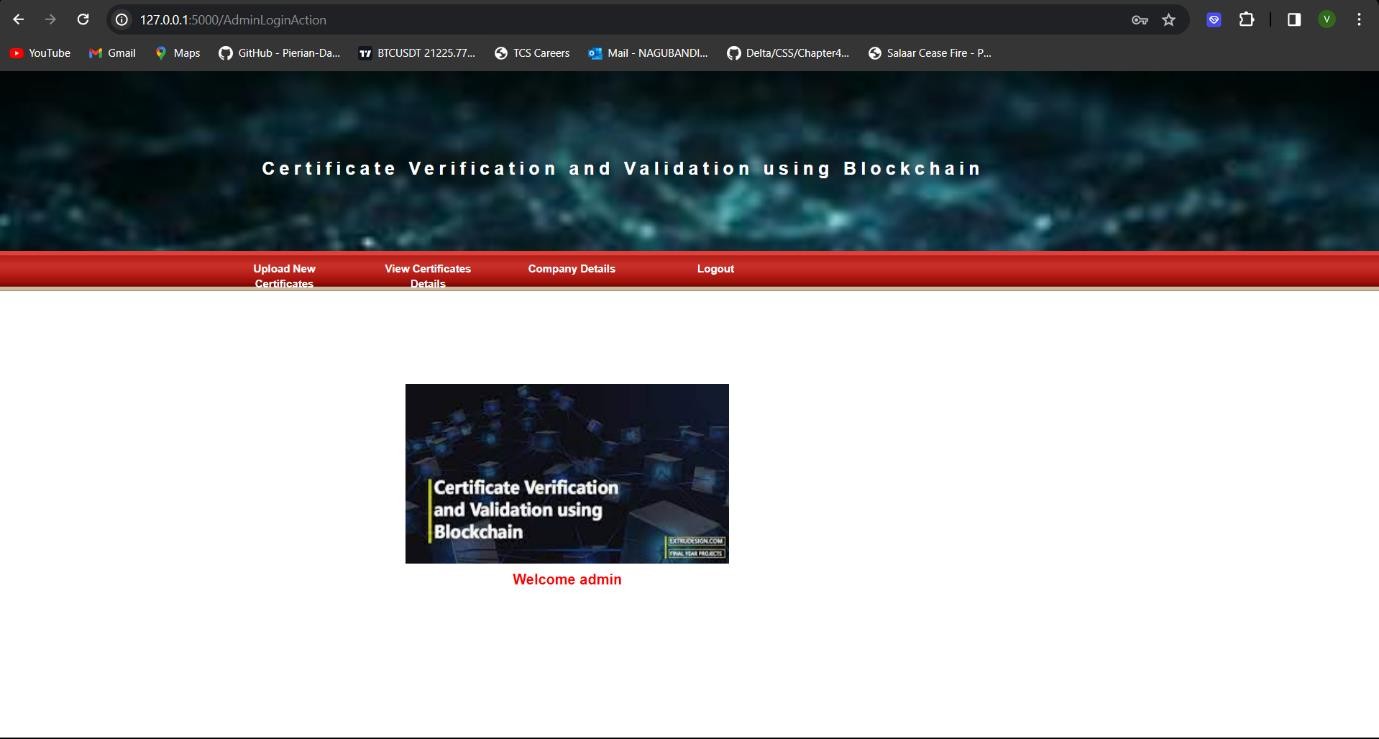
* In /AuthenticateScan, provide a mechanism for users to scan a QR code using their device camera or upload an image.
* Extract the data encoded in the QR code, which could be the certificate ID or a unique identifier.
* Authenticating Data:
* In /AuthenticateScanAction, call the readDetails function with the extracted data from the QR code.
* Validate the retrieved certificate information against known records or blockchain data.
* Based on the validation results, display a confirmation message or an error message on the AuthenticateScan.html template.

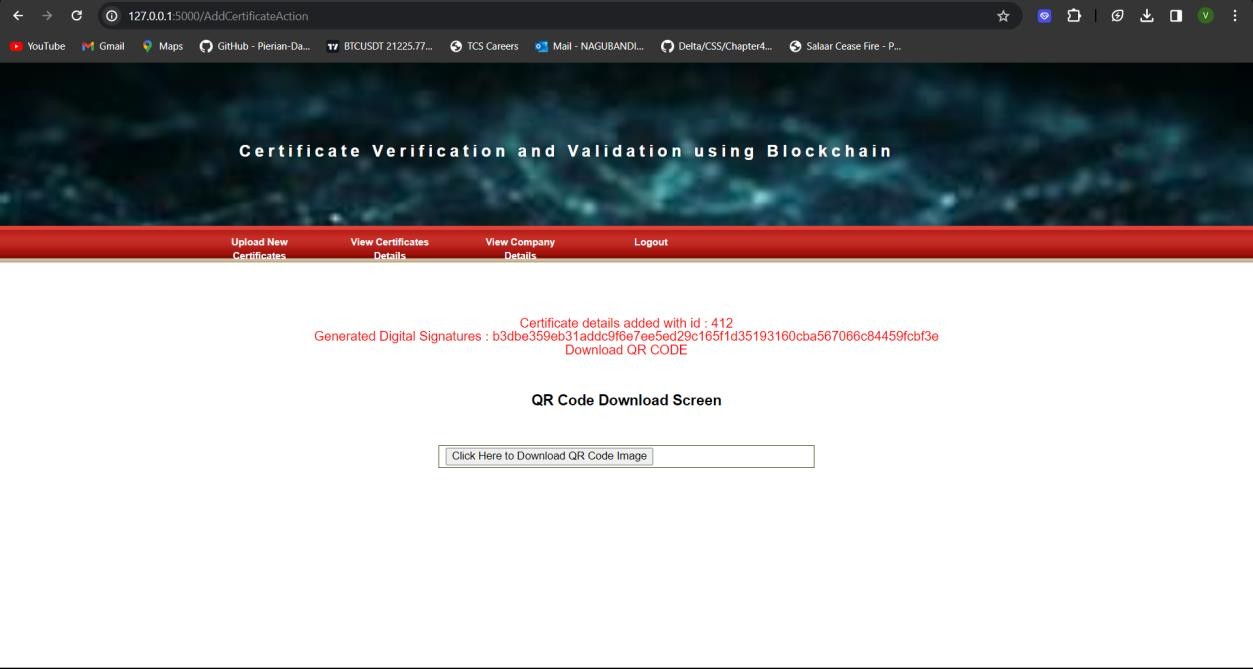
### Run the Application:

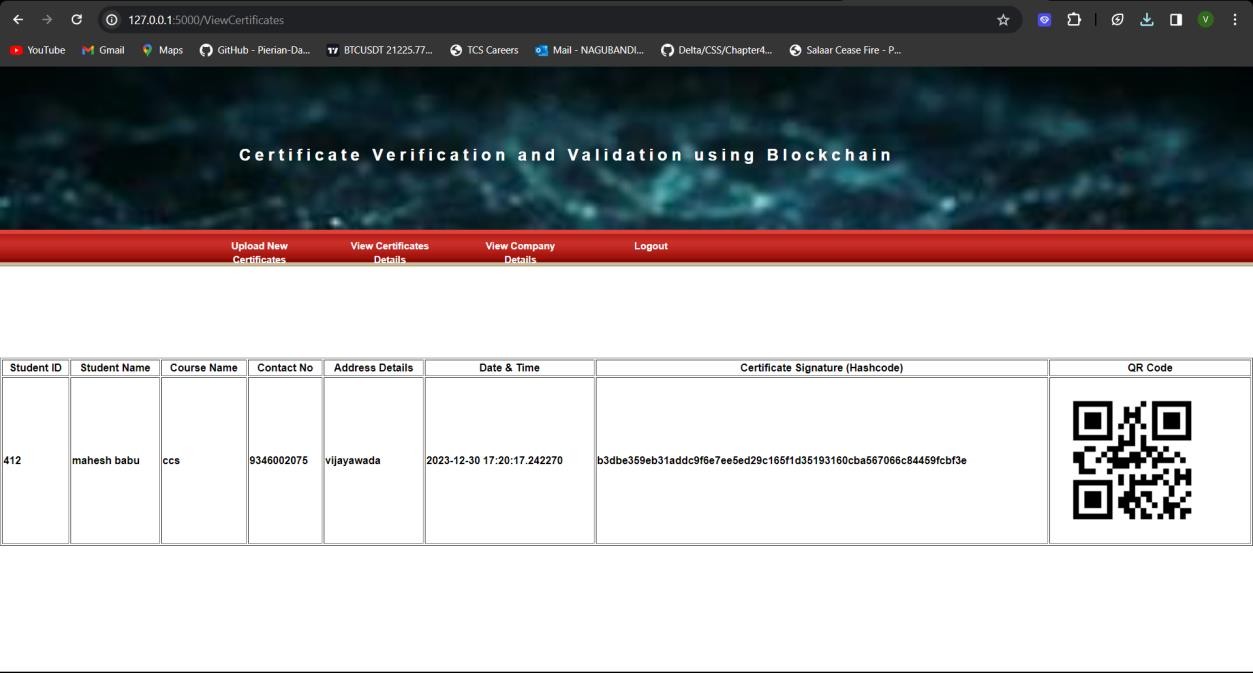
* + If the script is being executed directly (not imported as a module):
  + Start the Flask application using app.run()

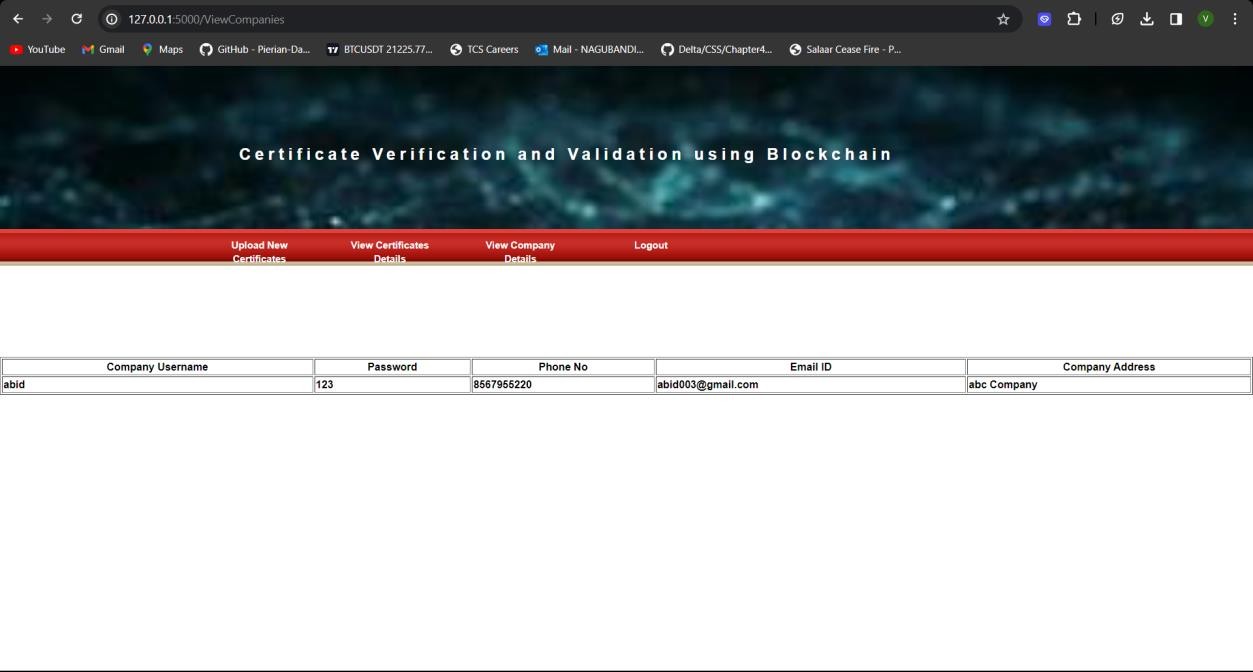
# APPENDIX-B SCREENSHOTS

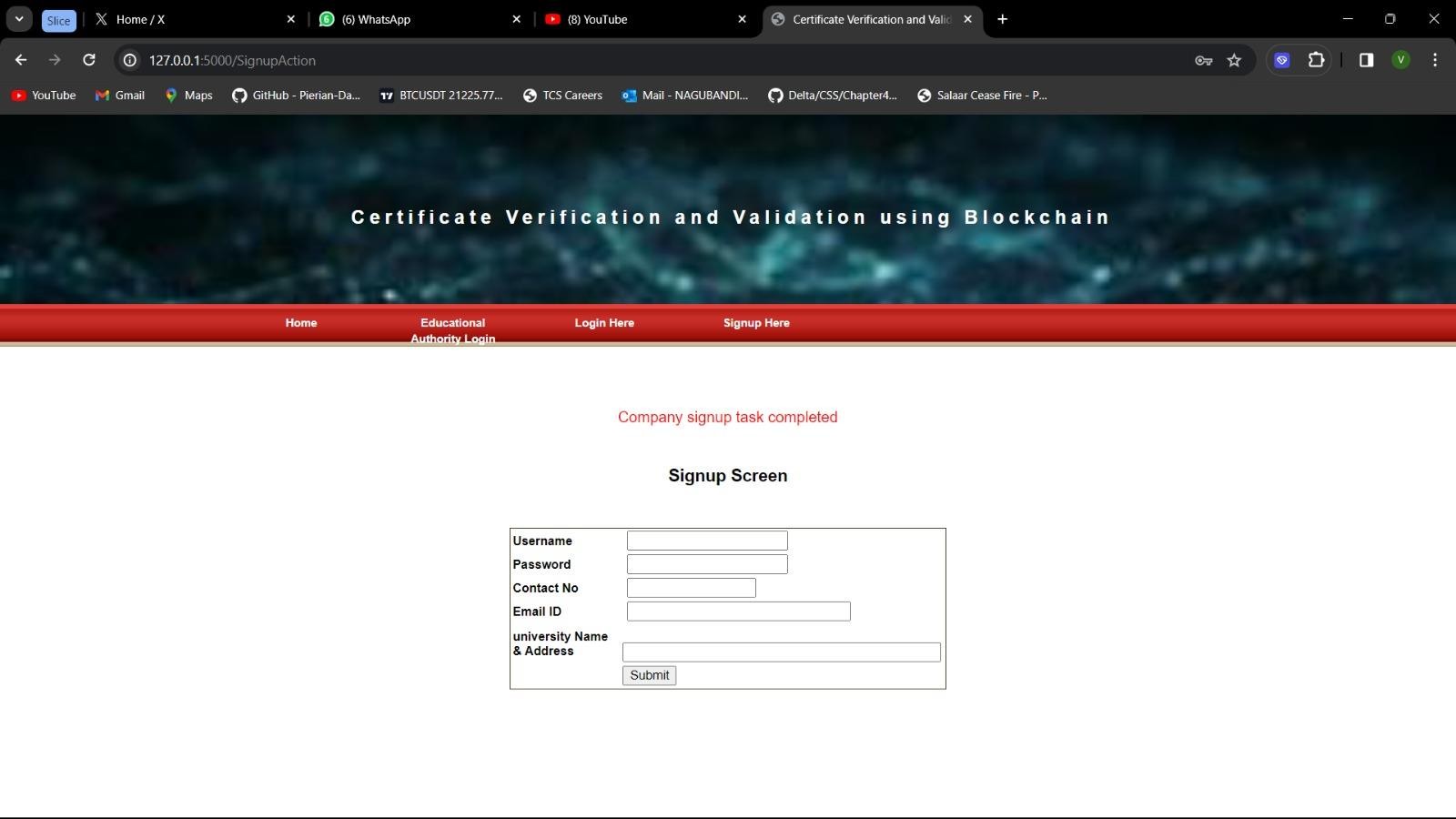
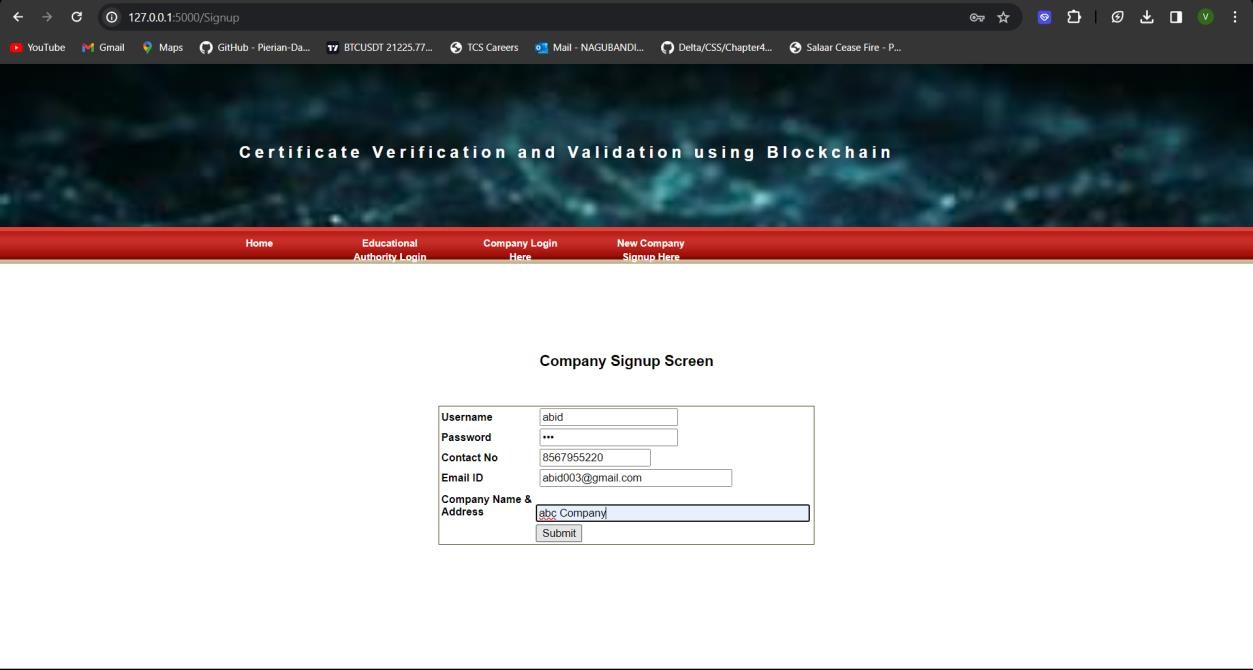


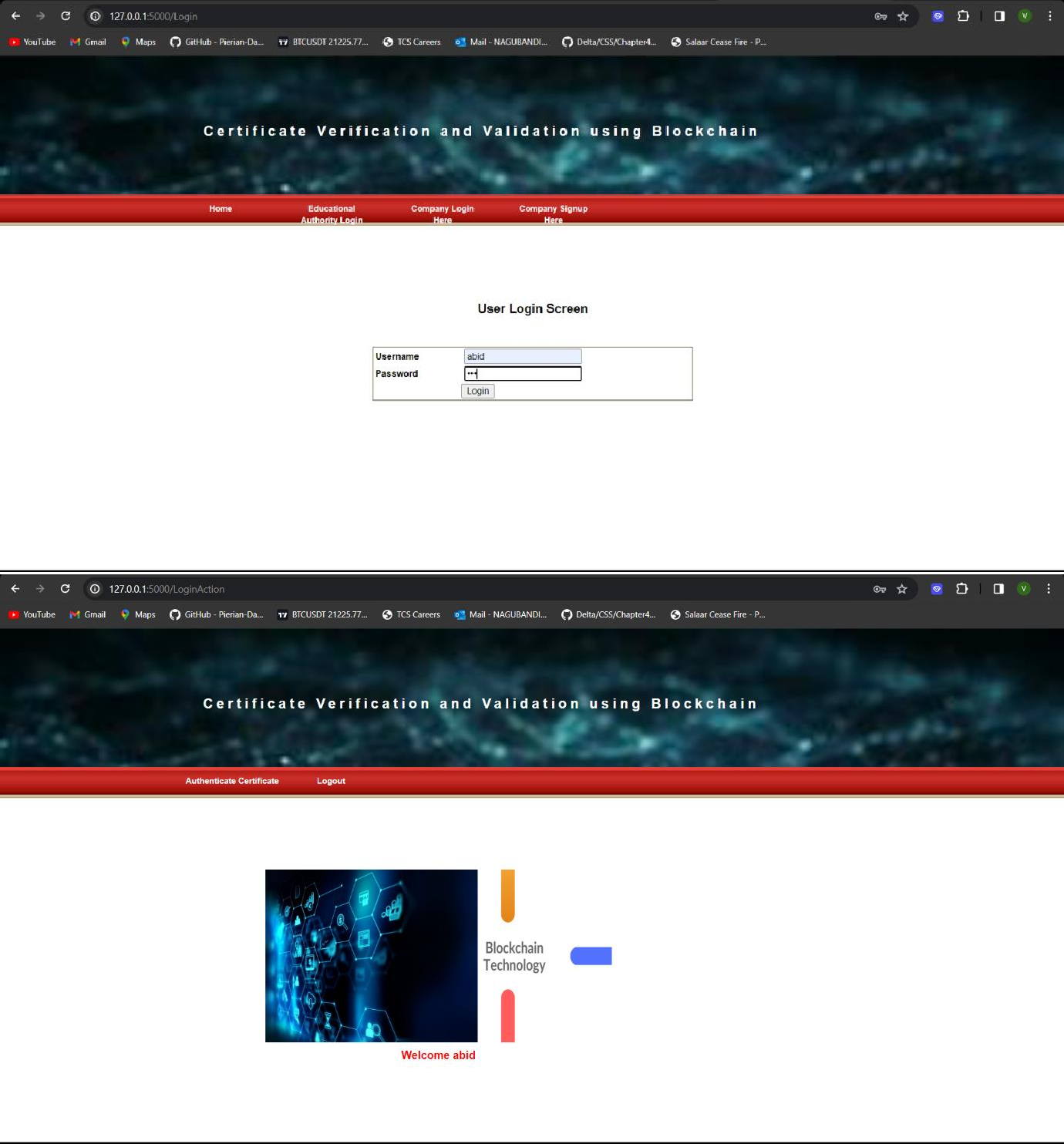


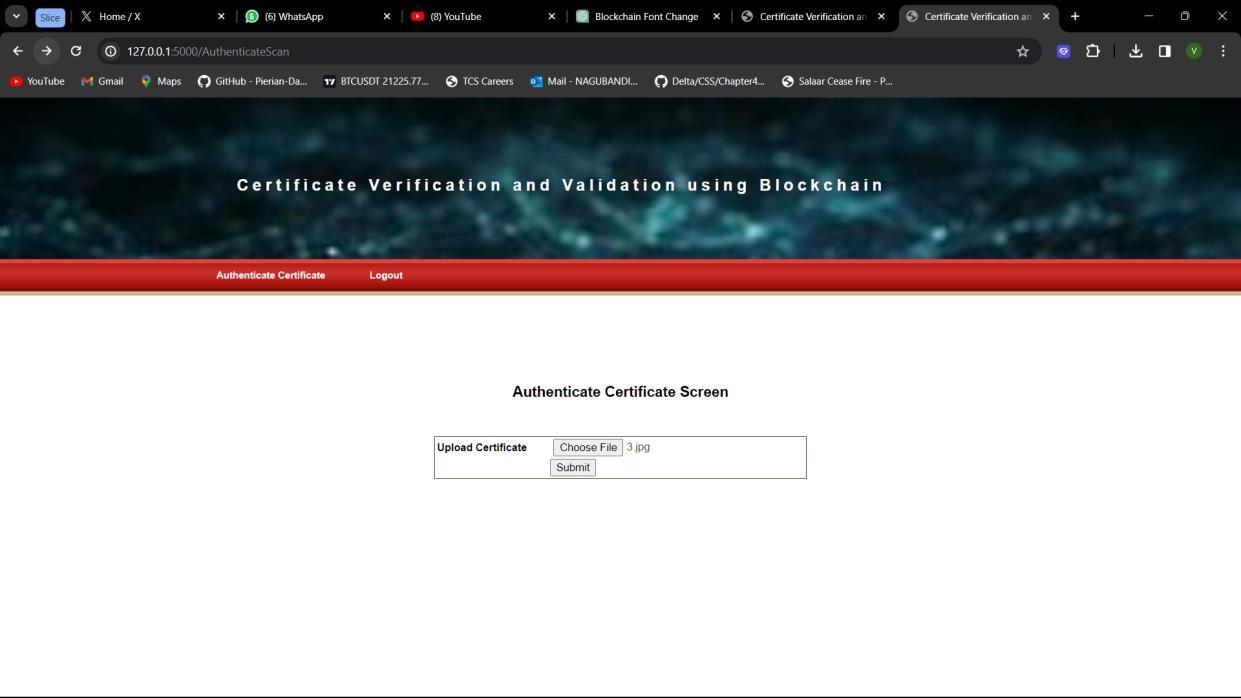




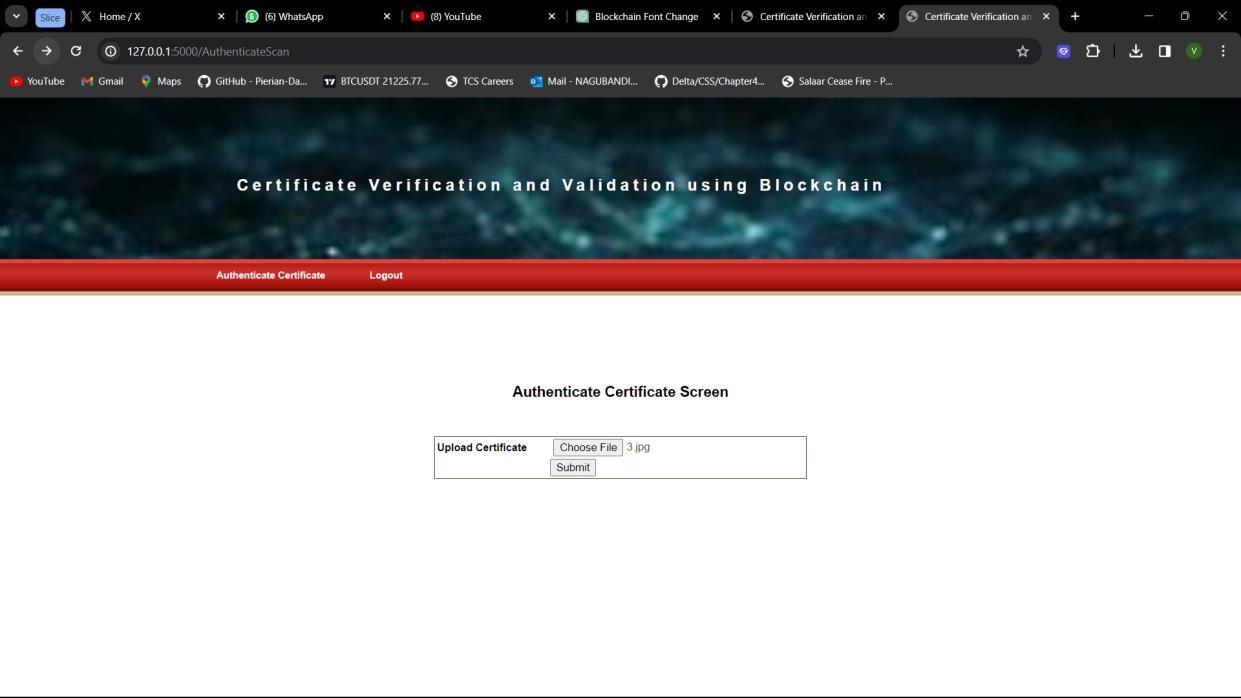


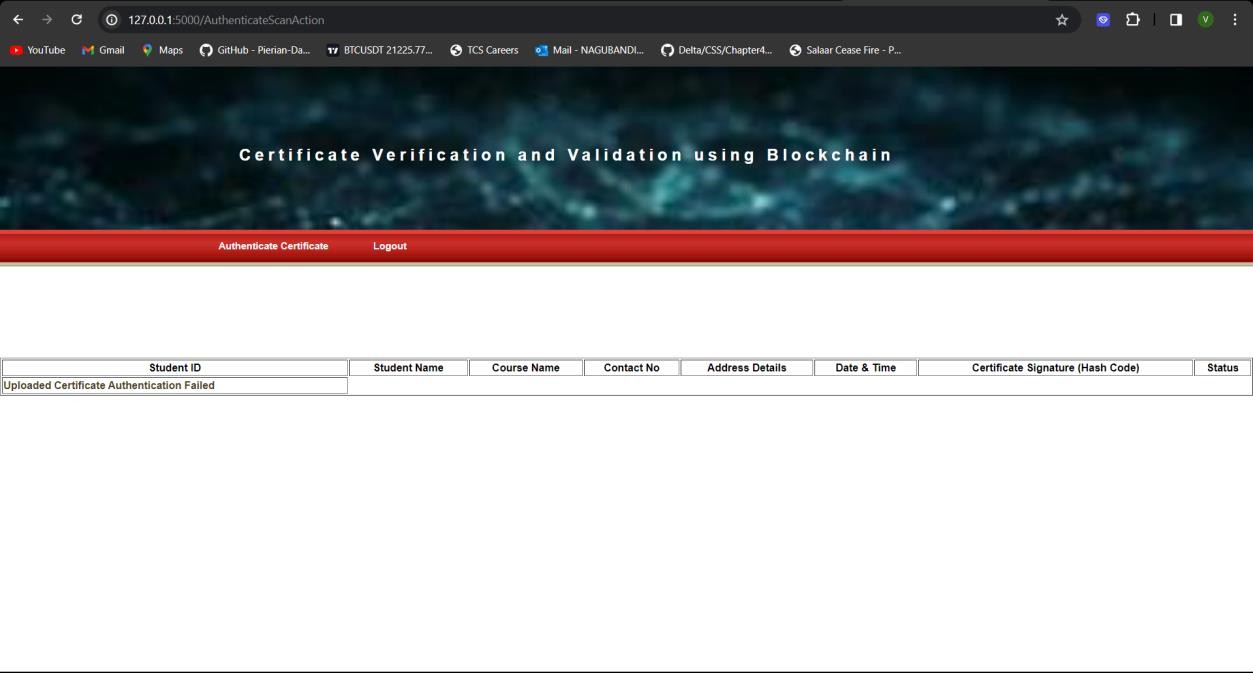


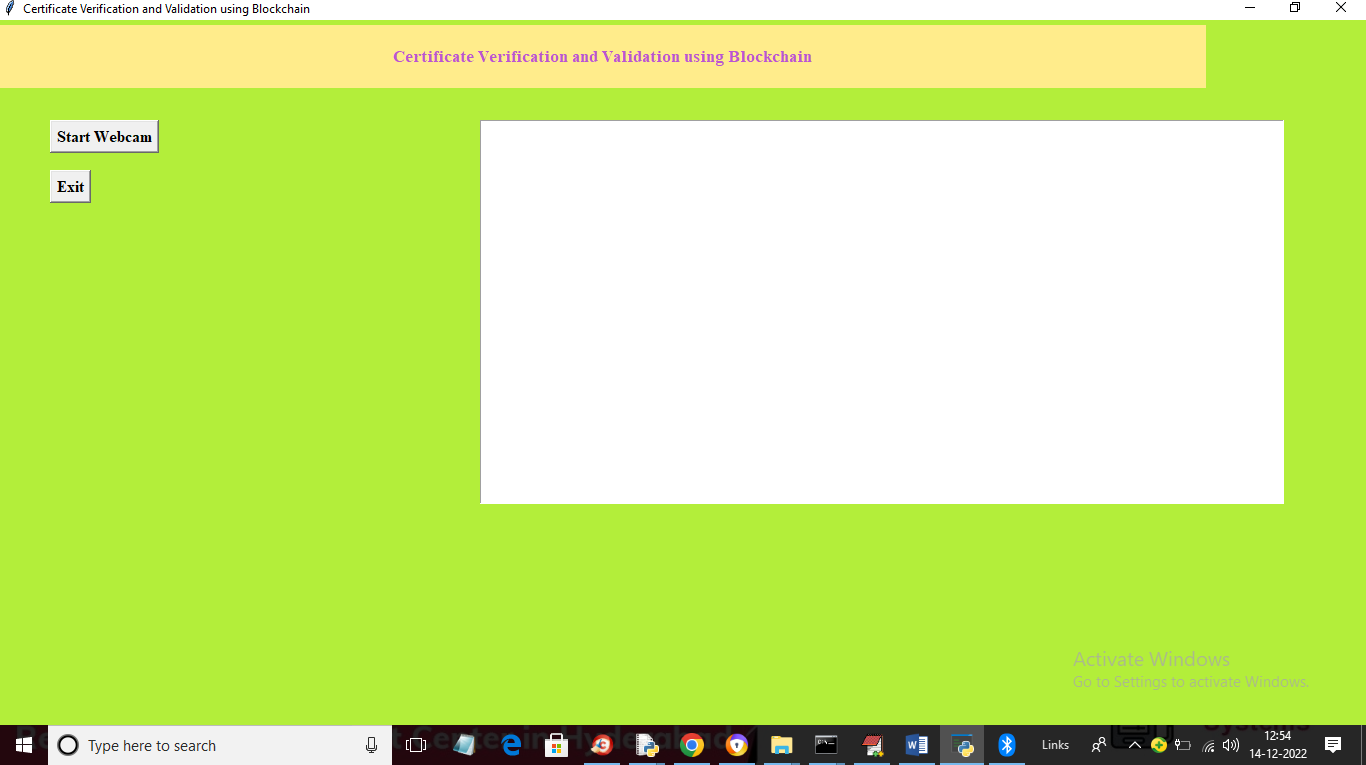


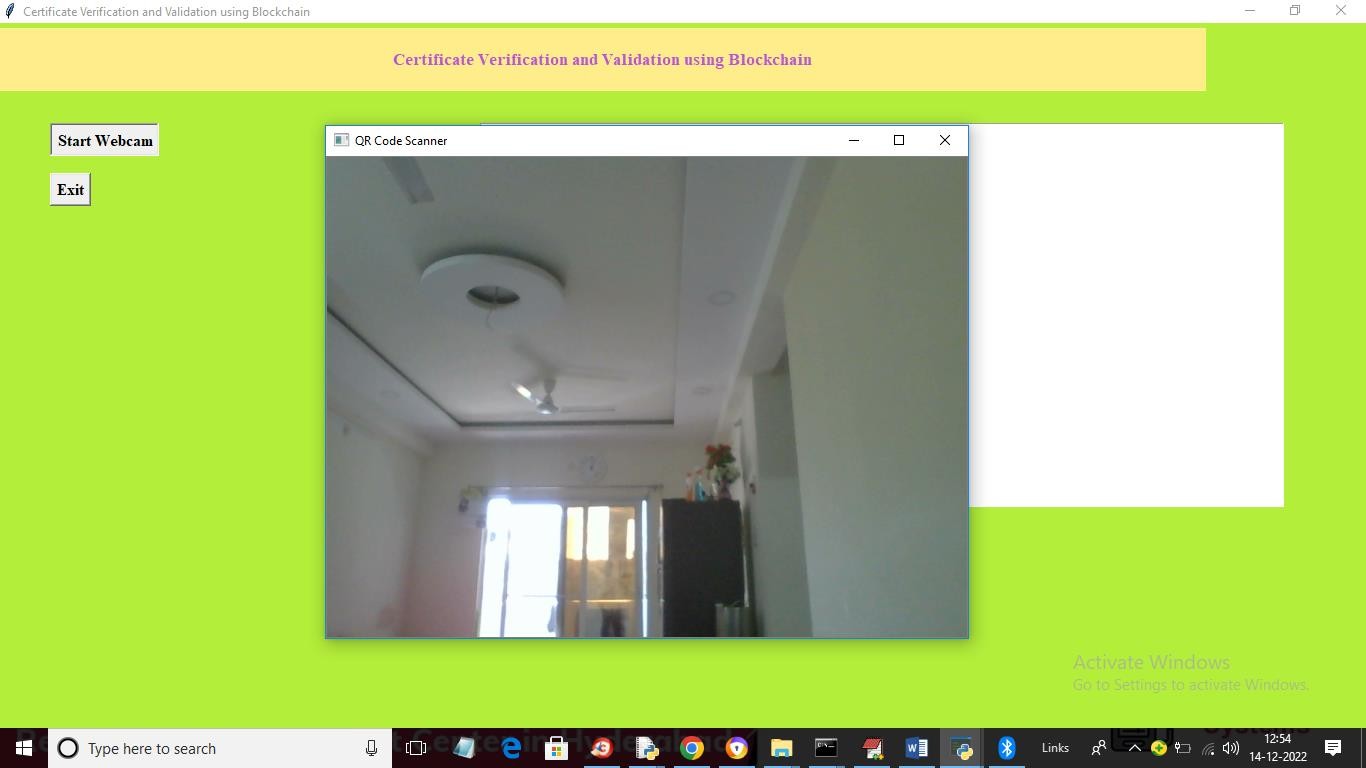


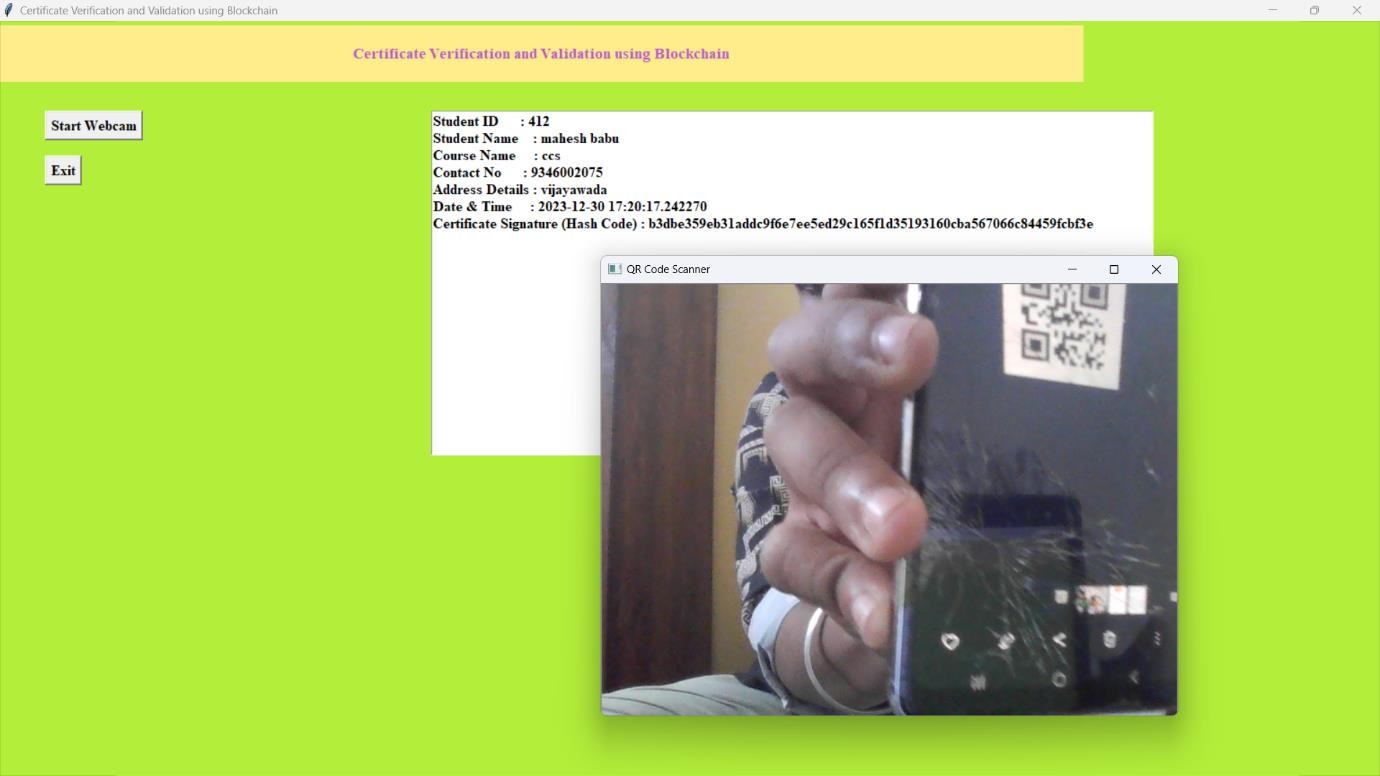


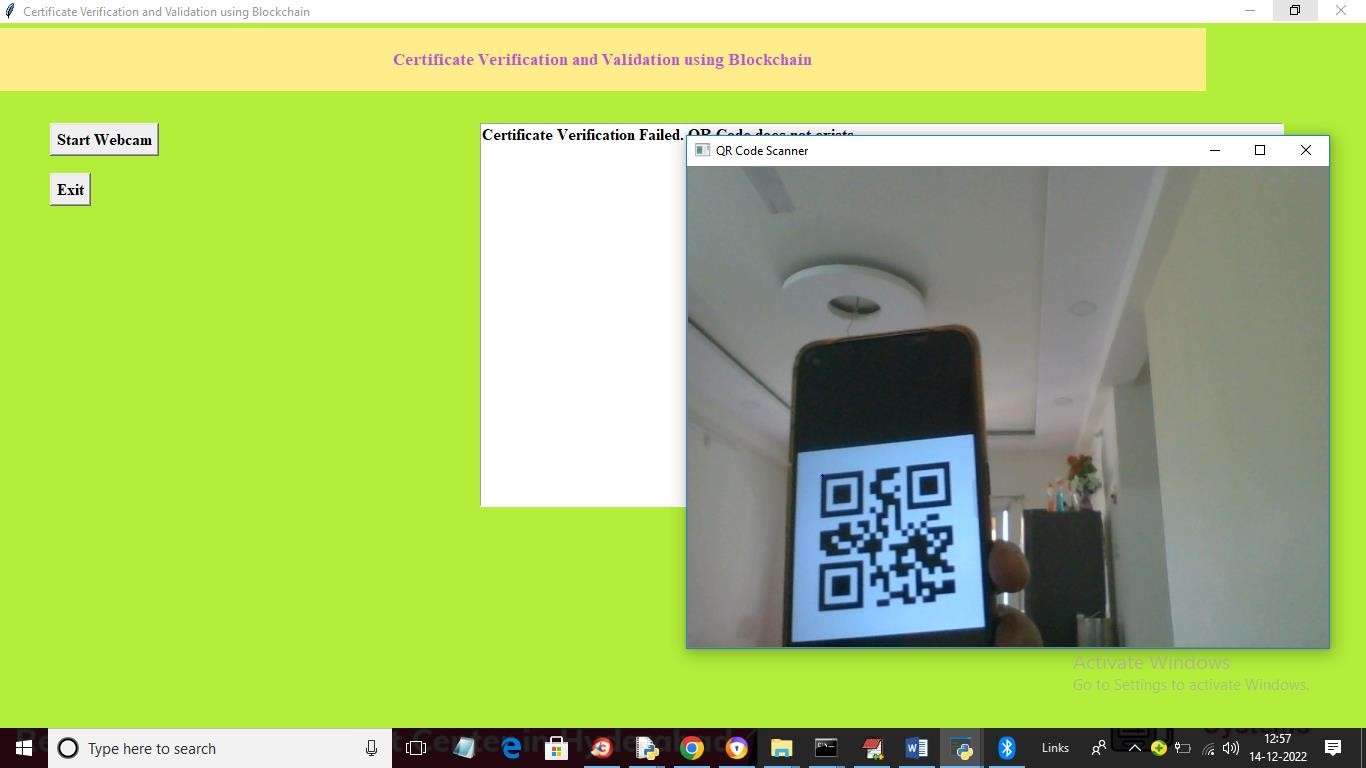






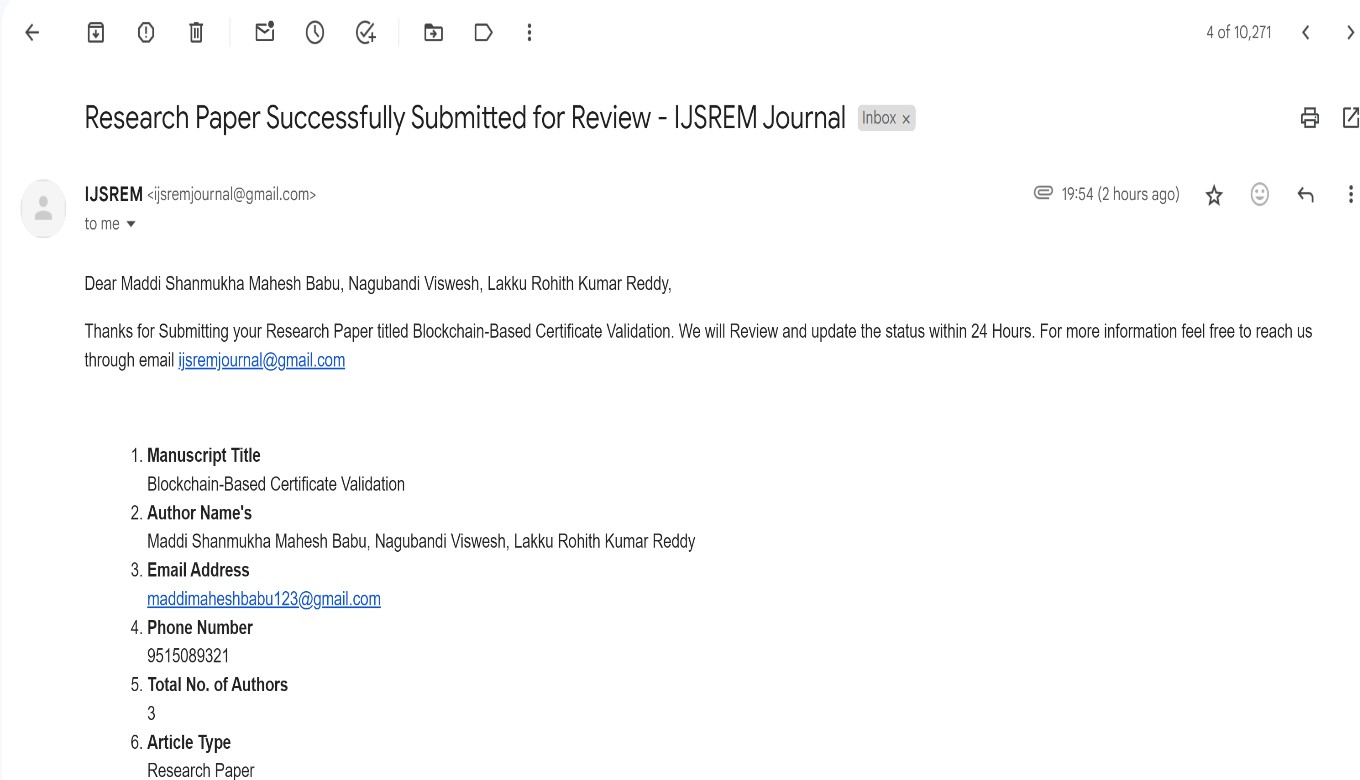






**APPENDIX-C ENCLOSURES**

# Conference Paper Presented Certificates of all students.



1. **Include certificate(s) of any Achievement/Award won in any project related event.**

****

# Research Paper ID: IJSREM28045

# The Research Paper issued by the "Internal Journal of Scientific Research In

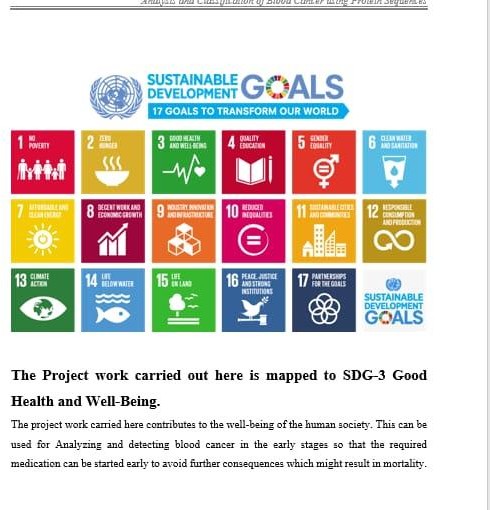
# Engineering & Management (IJSREM)" comes under UGC care.

# Publishing Authors Are:

# Maddi Shanmukha Mahesh Babu, Nagubandi Viswesh, Lakku Rohith Kumar Reddy

# Similarity Index / Plagiarism Check report clearly showing the Percentage (%). No need of page-wise explanation.





## The project work carried out here is mapped to SDG-4 Quality Education.

Our project aligns with Sustainable Development Goal 4 (Quality Education) by addressing the need for a secure and transparent certificate verification system. Through the implementation of blockchain technology, we contribute to ensuring the legitimacy of educational credentials. By enhancing the security and dependability of certificate verification processes, our project supports the goal of providing inclusive and equitable quality education for all.