A Project Report on

Comprehensive Certificate Validation and Verification System for Educational Institute using Blockchain

Submitted in partial fulfillment of the requirements for the award
of the degree of

Bachelor of Engineering

in

Information Technology

by

Sakshi Balekar (20104103)
Sarthak More (20104116)
Prathamesh Lambate (20104064)
Jaykumar Nayi (20104005)

Under the Guidance of

Mr. Mandar Ganjapurkar

Department of Information Technology
NBA Accredited
A.P. Shah Institute of Technology
G.B.Road,Kasarvadavli, Thane(W)-400615
UNIVERSITY OF MUMBAI

Academic Year 2023-2024

Approval Sheet

This Project Report entitled ***"Comprehensive Certificate Validation and Verification System for Educational Institute using Blockchain"*** Submitted by ***"Sakshi Balekar"(20104103), "Sarthak More"(20104116), "Prathamesh Lambate" (20104064), "Jaykumar Nayi"(20104005)*** is approved for the partial fulfillment of the requirement for the award of the degree of ***Bachelor of Engineering***in***Information Technology*** from ***University of Mumbai***.

(Mr. Mandar Ganjapurkar)
Guide

Dr. Kiran Deshpande
HOD, Information Technology

Place: A.P.Shah Institute of Technology, Thane
Date:

CERTIFICATE

This is to certify that the project entitled ***"Comprehensive Certificate Validation and Verification System for Educational Institute using Blockchain"*** submitted by ***"Sakshi Balekar"(20104103), "Sarthak More"(20104116), "Prathamesh Lambate"(20104064), "Jaykumar Nayi"(20104005)*** for the partial fulfillment of the requirement for award of a degree ***Bachelor of Engineering*** in ***Information Technology***, to the University of Mumbai, is a bonafide work carried out during academic year 2023-2024.

(Mr. Mandar Ganjapurkar)
Guide

Dr. Kiran Deshpande HOD, Information Technology	Dr. Uttam D.Kolekar Principal

External Examiner(s)	Internal Examiner(s)
1.	1.
2.	2.

Place: A.P.Shah Institute of Technology, Thane
Date:

Acknowledgement

We have great pleasure in presenting the report on **Comprehensive Certificate Validation and Verification System for Educational Institute using Blockchain** We take this opportunity to express our sincere thanks towards our guide **Mr. Mandar Ganjapurkar** for providing the technical guidelines and suggestions regarding the line of work. We would like to express our gratitude towards his constant encouragement, support, and guidance through the development of a project. We thank **Dr. Kiran B. Deshpande** Head of Department for his encouragement during the progress meeting and for providing guidelines to write this report. We express our gratitude towards BE project co-ordinator **Mr. Vishal Badgujar**, for being encouraging throughout the course and for their guidance. We also thank the entire staff of APSIT for their invaluable help rendered during the course of this work. We wish to express our deep gratitude towards all our colleagues of APSIT for their encouragement.

Sakshi Balekar
(20104103)

Sarthak More
(20104116)

Prathamesh Lambate
(20104064)

Jaykumar Nayi
(20104005)

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, We have adequately cited and referenced the original sources. We also declare that We have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Sakshi Balekar (20104103)

Sarthak More (20104116)

Prathamesh Lambate (20104064)

Jaykumar Nayi (20104005)

Date:

Abstract

This paper presents an innovative solution that utilizes blockchain technology, specifically Ethereum, to enhance the validation and verification of educational certificates. Traditional methods of certificate management often encounter issues such as fraud, inefficiency, and a lack of transparency. In response, this proposed system introduces a Comprehensive Certificate Validation and Verification System (CVVS) that aims to revolutionize the process. By leveraging the decentralized and immutable nature of blockchain, along with Ethereum's smart contract capabilities, the system ensures the authenticity and integrity of educational certificates. Key features of the system include decentralized issuance, tamper-proof record-keeping, secure verification, transparency, and fraud prevention. This forward-thinking approach seeks to streamline certificate management, build trust among stakeholders, and address the challenges that educational institutions face worldwide.

Contents

1 Introduction **1**
1.1 Motivation . . . 2
1.2 Problem Statement . . . 3
1.3 Objectives . . . 4
1.4 Scope . . . 5

2 Literature Review **6**

3 Project Design **8**
3.1 Existing System . . . 8
3.2 Proposed System . . . 10
3.2.1 Critical Components of System Architecture . . . 12
3.3 System Diagrams . . . 13
3.3.1 Use Case Diagram . . . 13
3.3.2 Flow Diagram . . . 15

4 Project Implementation **18**
4.1 Code Snippets . . . 18
4.2 Steps to access the System . . . 23
4.3 Timeline Sem VIII . . . 24

5 Testing **26**
5.1 Software Testing . . . 26
5.2 Functional Testing . . . 26

6 Result and Discussions **31**

7 Conclusion **37**

8 Future Scope **38**

Bibliography **39**
Appendix-A . . . 40
Appendix-B . . . 41

Publication **43**

List of Figures

3.1 Existing System . . . 8
3.2 System Architecture . . . 10
3.3 UCD 1 . . . 13
3.4 UCD 2 . . . 13
3.5 UCD 3 . . . 14
3.6 DFD Level 0 . . . 15
3.7 DFD Level 1 . . . 15
3.8 DFD Level 2 . . . 16

4.1 Creating Flask Application . . . 18
4.2 Compile Smart Contract . . . 19
4.3 Deploy Smart Contract . . . 20
4.4 Define Templates Values . . . 21
4.5 Transaction Process . . . 22
4.6 Ganntt Chart 01 . . . 24
4.7 Ganntt Chart 02 . . . 24
4.8 Ganntt Chart 03 . . . 25
4.9 Ganntt Chart 04 . . . 25

5.1 Test Case 01 (Login & signup) . . . 27
5.2 Test Case 02 (Certificate Generation) . . . 28
5.3 Test Case 03 (Verify Certificates) . . . 28
5.4 Test Case 04 (Validating Certificates) . . . 29
5.5 Test Case 05 (External verifier verify certificates) . . . 29
5.6 Certificate Verification Unsuccessful . . . 30

6.1 Login Page . . . 31
6.2 Student Dashboard Page . . . 31
6.3 Student Profile Page . . . 32
6.4 Student Marksheets Page . . . 32
6.5 Student Certificates Page . . . 33
6.6 Certificate Generation Page . . . 33
6.7 Marksheet Generation Page . . . 34
6.8 Generate Marksheet . . . 34
6.9 Generate Certificates Page . . . 35
6.10 Certificate Template . . . 35
6.11 Marksheet Template 1 . . . 36
6.12 Marksheet Template 2 . . . 36

8.1 Paper Publication 43
8.2 Paper Presentation 44

List of Tables

5.1 Functional Testing 27

List of Abbreviations

CVVS:	Certificate Verification and Validation System
SC:	Smart Contracts
IPFS:	Inter Planetary File System
EV:	External Verifier
DApp:	Decentralized Application

Chapter 1

Introduction

Ensuring the legitimacy and validity of academic credentials is a significant concern in today's educational landscape, affecting educational institutions, businesses, and individuals. However, traditional methods of certificate validation and verification are often inefficient, vulnerable to fraud, and lack transparency. To address these issues, blockchain technology, particularly Ethereum, presents a promising solution. This paper proposes the development of a Comprehensive Certificate Validation and Verification System (CVVS) specifically tailored for educational institutions, to revolutionize the certificate management process.

Blockchain technology, popularized by cryptocurrencies like Bitcoin and Ethereum, offers a secure, decentralized, and immutable ledger that records transactions. By leveraging blockchain, educational institutions can address issues related to certificate management, including counterfeit credential risks, administrative burdens, and reliance on centralized authorities for verification. By integrating Ethereum smart contracts, the proposed CVVS can automate and streamline the issuance, validation, and verification of educational certificates, while ensuring transparency, security, and trustworthiness.

Our paper focuses on leveraging the Ethereum blockchain technology to design and implement a CVVS for educational institutions. It will explore the underlying principles of blockchain, Ethereum smart contracts, and their application in the context of certificate management. Additionally, the paper will discuss the potential benefits of adopting such a system, including enhanced security, efficiency gains, reduced administrative overhead, and increased trust among stakeholders.

In general, CVVS represents a paradigm shift in how academic credentials are managed and authenticated. This system harnesses the power of blockchain technology, particularly Ethereum, to ensure more secure, transparent, and efficient credential verification, paving the way for a more secure, transparent, and efficient credentialing ecosystem.

1.1 Motivation

The purpose of implementing a Comprehensive Certificate Validation and Verification System for Educational Institutes with Blockchain is to address several pressing issues and to benefit educational institutions:

- **Rising Education Fraud:** In recent years, there has been a significant increase in the number of individuals presenting fraudulent educational credentials. This not only undermines the value of legitimate educational qualifications but also poses a risk to employers who may unknowingly hire candidates with misrepresented or counterfeit degrees. This system can serve as a deterrent against such fraudulent activities by providing secure and tamper-proof verification.
- **Inefficient Verification Process:** The traditional process of verifying academic certificates is time-consuming and often involves manual checks and communication between educational institutions and employers. This can lead to delays in hiring and administrative burdens for both educational institutions and employers. A blockchain-based system offers a streamlined and instant verification process.
- **Data Security and Privacy:** Educational records are sensitive and confidential, and maintaining their security and privacy is of utmost importance. Traditional methods, such as paper certificates, are susceptible to theft, loss, or unauthorized access. A blockchain system enhances data security and privacy, as it provides robust encryption and access controls.
- **Transparency and Trust:** The transparency of blockchain technology ensures that all relevant parties have access to the same, unalterable records. This fosters trust between educational institutions, students, and employers. Transparency also makes it easier to spot any inconsistencies or inaccuracies in academic credentials.
- **Technology Advancements:** As technology continues to advance, it's essential for the education sector to adapt and harness these innovations. Blockchain technology represents a cutting-edge solution that aligns with the digital transformation happening across various industries.

1.2 Problem Statement

The Comprehensive Certificate Validation and Verification System for Educational Institutes using Blockchain is developed to address a range of critical issues and challenges within the current education and certification ecosystem. These problems encompass:

- **Certificate Fraud and Counterfeiting:** One of the most significant problems in the education sector is the prevalence of fake or forged certificates. With traditional paper-based certifications, it is relatively easy for individuals to produce counterfeit documents. This leads to the devaluation of legitimate qualifications and can have severe consequences for employers and academic institutions.

- **Inefficient Verification Process:** The process of verifying academic credentials is often slow and cumbersome. Employers, educational institutions, and other relevant parties may need to manually contact universities or schools to verify the authenticity of certificates, resulting in delays in hiring and other processes.

- **Credential Verification Costs:** Manual verification processes are not only time-consuming but also incur significant costs. Educational institutions and employers must allocate resources to verify certificates, and these expenses can add up over time.

- **Lack of Transparency:** In some instances, educational institutions may lack transparency in their certification processes. This lack of transparency can lead to doubts regarding the legitimacy of certificates, further exacerbating the problem of certificate fraud.

- **Global Verification Challenges:** As education becomes increasingly globalized, verifying international qualifications can be particularly challenging due to differences in verification methods and institutions' reputations.

- **Time-Consuming Credential Retrieval:** Graduates often need to request physical copies of their certificates from educational institutions, which can be time-consuming and inconvenient.

- **Inconsistencies in Records:** Discrepancies or errors in academic records can lead to complications when certificates are validated. These inaccuracies may be unintentional but still pose challenges in the verification process.

1.3 Objectives

1. Develop a secure and decentralized system for issuing, storing, and validating educational certificates using blockchain technology, specifically leveraging the Ethereum platform.

2. Implement Ethereum smart contracts to automate the certificate issuance process, ensuring that certificates are tamper-proof, immutable, and transparently recorded on the blockchain.

3. To Enhance the security and integrity of educational certificates by leveraging cryptographic techniques and consensus mechanisms inherent in blockchain technology.

4. Streamline the certificate validation and verification process for educational institutes, employers, and other stakeholders, reducing reliance on centralized authorities and mitigating the risk of fraudulent credentials.

5. Improve efficiency and reduce administrative overhead associated with certificate management through the automation and digitization of processes enabled by the proposed system.

6. Foster trust and transparency within the educational ecosystem by providing a reliable and auditable source of truth for certificate authenticity and validation.

7. Facilitate seamless interoperability with existing educational systems and databases, ensuring smooth integration and adoption of the Comprehensive Certificate Validation and Verification System (CVVS).

8. Conduct thorough testing and validation of the CVVS to ensure its reliability, scalability, and usability in real-world educational environments.

1.4 Scope

1. The project will focus on integrating blockchain technology, particularly Ethereum, into the existing infrastructure of educational institutes to facilitate certificate validation and verification.

2. The system will cover the entire certificate issuance process, from the generation of certificates by educational institutes to their registration and storage on the blockchain.

3. Development of Ethereum smart contracts will be a key component, automating various aspects of certificate management, such as issuance, validation rules, and expiry conditions.

4. Designing user-friendly interfaces for educational institutes, certificate holders, and validators to interact with the system, making the process intuitive and accessible.

5. The system will be designed to seamlessly integrate with existing educational management systems and databases, enabling smooth data exchange and interoperability.

6. Enable students and graduates to access their digital certificates conveniently and securely through the web interface.

7. Provide an intuitive and responsive design that works seamlessly across various devices and browsers.

Chapter 2

Literature Review

In paper [1], titled “A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification”, authored by A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, published in IEEE 2023. The author aims to compile all relevant research into a systematic literature review, highlighting key contributions from various researchers throughout the year. They have identified 34 relevant studies out of the 1744 papers published between 2018 and 2022 by employing the PRISMA framework. Three research questions were developed to outline the scope of the review. The following six themes were found using qualitative analysis of the reviewed papers: blockchain categorization, automatic certificate (diploma) generation, security and transparency, adapting existing architectures, and blockchain technology. Despite a growing interest, only 34 articles met the rigorous criteria for final investigation. It focuses on the adoption of blockchain for verifying academic credentials, particularly diplomas. Several challenges to the widespread adoption of blockchain for diploma verification were identified, including automation, immutability of smart contracts, maintenance costs, knowledge gaps, off-chain transfer, big data management, energy consumption, adaptability, and identity verification.

In paper [2], titled “A Blockchain-Based E-Commerce Reputation System Built With Verifiable Credentials”, authored by Ö. Doğan and H. Karacan, published in 2023. The proposed model has been developed into a software system and deployed on cloud servers. Performance evaluations indicate that the system is feasible and can be integrated into existing e-commerce ecosystems. The system is built on a permissioned blockchain, specifically Hyperledger Fabric. Integration of verifiable credentials such as digital identities, proofs of transactions, and feedback submissions makes the model innovative and robust. One of the key advantages of the proposed approach is the use of verifiable credentials for the digital identities of sellers, feedback tokens issued to buyers after performing an e-commerce transaction, and discount tokens issued to buyers after feedback submission. This helps to ensure that the feedback and identity information is authentic and tamper-proof, reducing the likelihood of identity-related attacks. Additionally, the collection of feedback and application of business rules are implemented as smart contracts on the Hyperledger Fabric blockchain. This provides a secure and transparent mechanism for processing feedback, reducing the likelihood of unfair feedback.

In paper [3], titled “Academic Certificate Validation Using Blockchain Technology”, authored by G. Sethia, S. Namratha, S. H, and S. C. S, published in 2022. The review analyzed the practical applications of blockchain technology in various activities, highlighting correlations among features in different educational applications. Researchers should focus on subjects like identity management, document management, certificate verification, healthcare, insurance, e-voting, supply chain management, and property management with blockchain technology. Physical anti-counterfeiting features deter tampering, while digital solutions enhance intelligence and identification of culprits, as well as enable convenient authentication. This proposal focuses on designing and implementing a system that will prove to be a solution for addressing the issue of fake certificates using Hyperledger Fabric. The technology here is tamper-proof and maintains transparency. This system will have a database of academic certificates awarded by the University, which is recorded as a transaction using the Hyperledger Fabric, which further can be referred by other organizations present in the network to verify the authenticity of the certificates using the information provided by the students to the database.

In paper [4], titled “Certificate Verification using Blockchain and Generation of Transcript”, authored by Devdoot Maji, Ravi Singh Lamkoti, Hitesh Shetty, Bharati Gondhalekar, published in 2021. The system automates the process of certificate generation, reducing the need for manual intervention. The certificate’s hash is stored on the blockchain, while the original document is stored in the InterPlanetary File System (IPFS). This dual storage approach ensures data preservation and fosters transparency in the verification process. The next issue that comes into the picture is the time consumption for validating certificates step-by-step. The technology used for solving these problems was IPFS and Ethereum Smart Contracts.

In paper [5], titled, “Blockchain Technology and Academic Certificate Authenticity”, authored by Rama Reddy, T., Prasad Reddy, P.V.G.D., Srinivas, R. et al., published in 2021. The review analyzed the practical applications of blockchain technology in various activities, highlighting correlations among features in different educational applications. Researchers should focus on subjects like identity management, document management, certificate verification, healthcare, insurance, e-voting, supply chain management, and property management to blockchain technology. Physical anti-counterfeiting features deter tampering, while digital solutions enhance intelligence and identification of culprits, as well as enable convenient authentication.

Chapter 3

Project Design

3.1 Existing System

The current system for storing certificates is centralized, which means that all certificate records are stored in a single location. However, the verification process for these certificates is manual, which is both time-consuming and prone to errors. This lack of automation can lead to inconsistencies in the verification process, and there is no guarantee that certificates are being verified accurately.

Another issue with the current system is that students often bring their certificates to interview places, which can compromise their security. There is no assurance that the certificates are being handled and stored properly, which can make them vulnerable to theft or loss. Overall, the lack of security measures for certificates is a significant concern that needs to be addressed to ensure that they are protected and trusted as valid credentials.

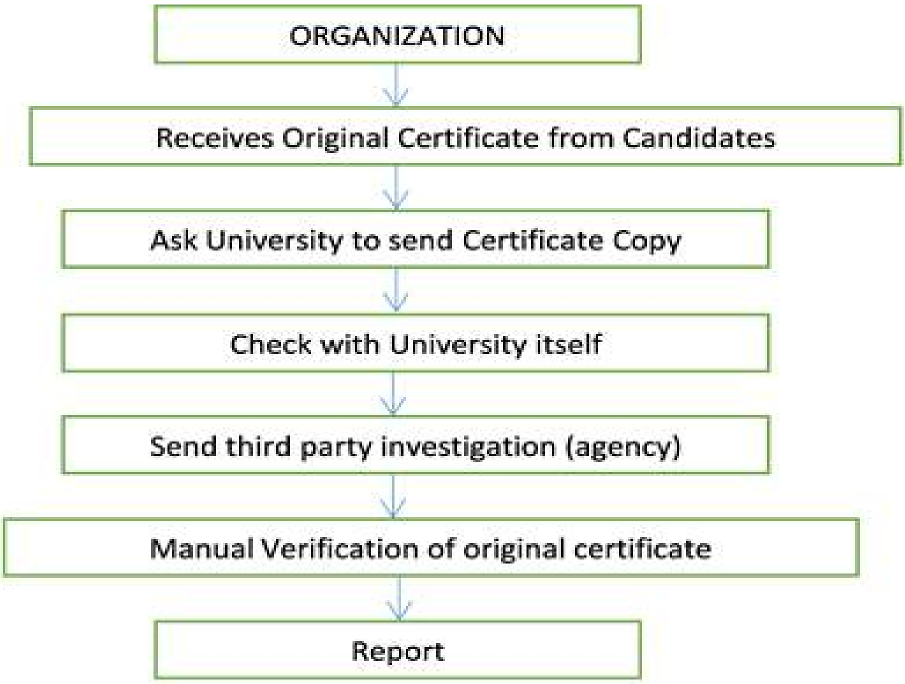

ORGANIZATION
Receives Original Certificate from Candidates
Ask University to send Certificate Copy
Check with University itself
Send third party investigation (agency)
Manual Verification of original certificate
Report

Figure 3.1: Existing System

- Receives Original Certificate from Candidates: The organization receives the physical certificate from the candidate.
- Ask University to send Certificate Copy: The organization then contacts the university that issued the certificate and requests a copy of the candidate's certificate for verification purposes.
- Check with the University itself: This step likely involves the organization directly verifying with the university whether the copy they received matches the original presented by the candidate.
- Send third-party investigation (agency): If further verification is required, the organization might outsource the verification process to a third-party agency specializing in certificate verification.
- Manual Verification of original certificate: The organization manually examines the original certificate for any signs of tampering or forgery.
- Report: Finally, the organization generates a report summarizing the results of the verification process.

To ensure the legitimacy of educational qualifications, organizations often implement a multi-step verification process. This typically involves collecting the original certificate from the candidate, requesting a copy directly from the issuing university for comparison, and potentially involving a third-party verification agency. The organization also manually inspects the original certificate for signs of forgery. Finally, a report is generated to document the verification's outcome.

3.2 Proposed System

This is a detailed explanation of a system architecture depicting a blockchain-based system that is designed for verification and validation purposes. The system involves three different user sides, namely Educator, Student, and Verifier (External Verifier). All user sides are connected through web applications that are developed using modern web technologies.
The users interact with the Ethereum Blockchain through the internet, which is hosted on a server that interacts with a database for storing user details and generated documents. The system is designed to enable Educators to create and issue certificates, students to receive and access certificates, and verifiers to verify and validate certificates.

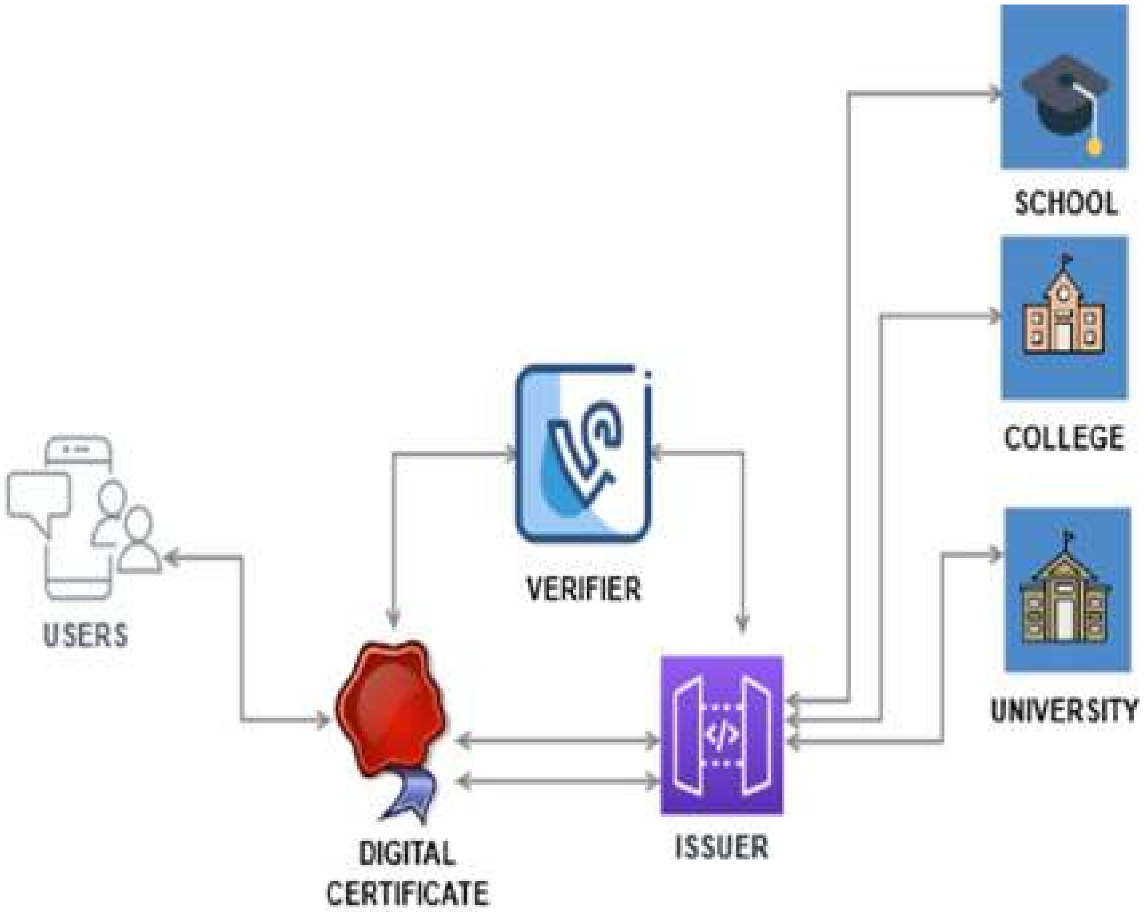


Figure 3.2: System Architecture

The system leverages smart contracts to implement the logic and rules for creating, issuing, verifying, validating, revoking, and renewing certificates. The database stores user details and generated documents, such as certificates, QR codes, and verification results.
This system provides a secure way of issuing and verifying certificates, thereby eliminating the need for traditional paper-based certificates. It ensures that the certificates are authentic and tamper-proof, making it an ideal solution for educational institutions and organizations that require a secure and reliable certification system.

- Faculty Issues Certificate: The faculty creates a digital certificate for the student and stores it on a blockchain ledger.
- Student Receives Digital Certificate: The student receives a copy of their digital certificate along with a unique identifier.
- Verifier Requests Certificate: The organization seeking to verify the certificate asks the student for the unique identifier.
- Verifier Checks Ledger: The organization uses the identifier to access the certificate on the blockchain ledger and verify its authenticity.

The process of issuing a digital certificate by the university starts with creating a unique certificate for the student which is then securely stored on a blockchain ledger. The student receives a copy of this digital certificate along with a unique identifier which is used for verification purposes. When an organization seeks to verify the certificate, it asks the student for the unique identifier. The organization then uses this identifier to access the certificate on the blockchain ledger and check its authenticity. This ensures that the certificate is tamper-proof and can be verified by any interested party.

3.2.1 Critical Components of System Architecture

1. **Smart Contracts:** Smart contracts are self-executing contracts with the terms of the agreement directly written into code. In the context of a certificate verification and validation system, smart contracts manage the issuance, storage, and verification of certificates on the blockchain. There are typically two main types of smart contracts involved:

   - Certificate Issuance Contract: This contract is responsible for creating and storing certificates on the blockchain. It defines functions for issuing new certificates, specifying certificate details, and storing them securely.
   - Certificate Verification Contract: This contract provides functions to verify the authenticity and validity of certificates stored on the blockchain. It retrieves certificate details and verifies their integrity when requested.

2. **Certificate Structure:** Define the structure of the certificates to be issued and verified. This includes fields such as certificate ID, recipient name, issuer name, issue date, expiration date, and any other relevant information. The structure should be standardized to ensure consistency and interoperability across certificates.

3. **Ethereum:** Ethereum supports Turing-complete smart contracts, which are self-executing contracts with the terms of the agreement directly written into code. Smart contracts enable the automation of certificate issuance, storage, and verification processes. By deploying smart contracts on Ethereum, certificate authorities can define rules for issuing certificates, store certificate data on the blockchain, and provide functions for verifying the authenticity of certificates.
   Ethereum provides a secure environment for executing smart contracts. The platform leverages cryptographic techniques such as hashing, digital signatures, and encryption to ensure the integrity, authenticity, and confidentiality of data. Certificate data stored on Ethereum is cryptographically secured, making it resistant to unauthorized access and tampering.

4. **Decentralized Application (DApp) Development:** Python frameworks like Flask or Django can be used to build decentralized applications (DApps) that provide user interfaces for interacting with the certificate verification system. These DApps can communicate with smart contracts deployed on the blockchain, allowing users to request, issue, and verify certificates through a web or mobile interface.

3.3 System Diagrams

3.3.1 Use Case Diagram

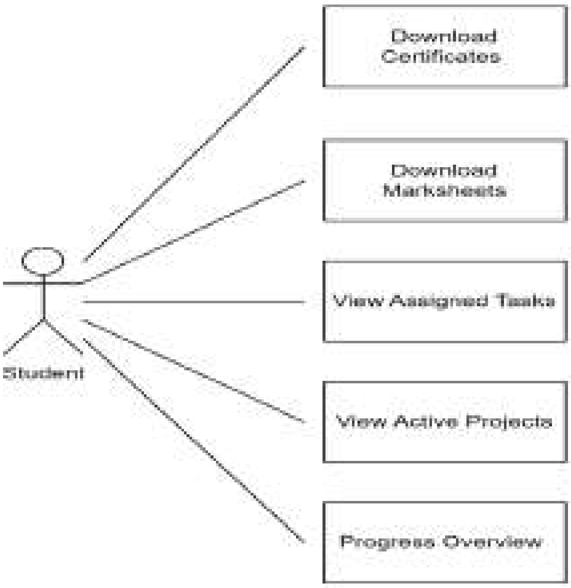


Figure 3.3: UCD 1

Our certificate verification and validation system offers students a comprehensive range of features. You can easily access and download your certificates and marksheets, and view the tasks assigned to you as well as the ongoing projects you're involved in. Moreover, you can track your progress and stay updated on your academic achievements.

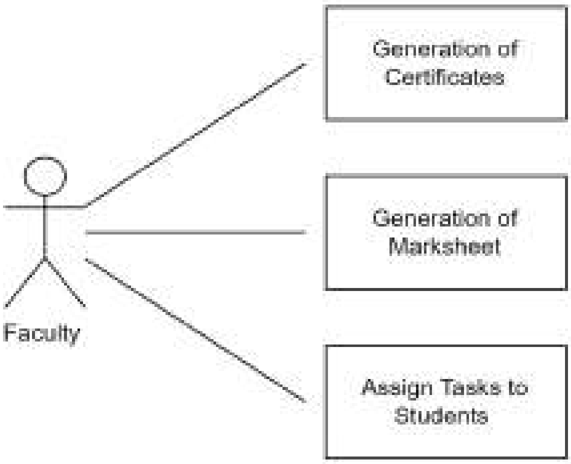


Figure 3.4: UCD 2

Our certificate verification and validation system enables faculty members to manage and monitor the certification process easily. With this system, faculty members can generate certificates and marksheets with ease and accuracy. In addition, the system allows faculty members to assign specific tasks to individual students, ensuring that all requirements are met for the successful completion of the certification process.

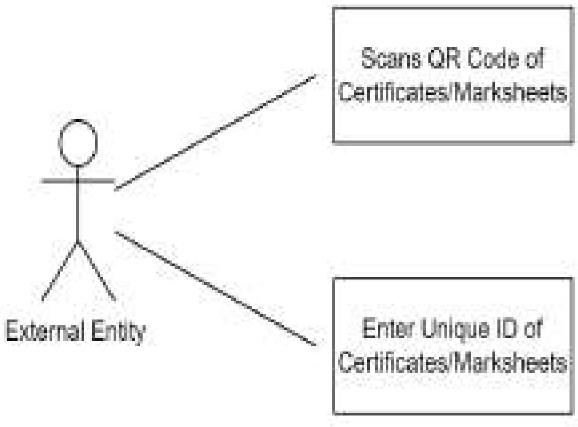

Scans QR Code of Certificates/Marksheets
External Entity
Enter Unique ID of Certificates/Marksheets

Figure 3.5: UCD 3

Our comprehensive and reliable certificate verification and validation system not only ensures the authenticity of a student's mark sheet or certificate but also provides access to external entities such as universities or institutes for verification purposes. This is achieved through the use of a QR code that is printed on the document or a unique ID that is assigned to the mark sheet or certificate. By using this system, external entities can easily and accurately verify the validity of a student's credentials.

3.3.2 Flow Diagram

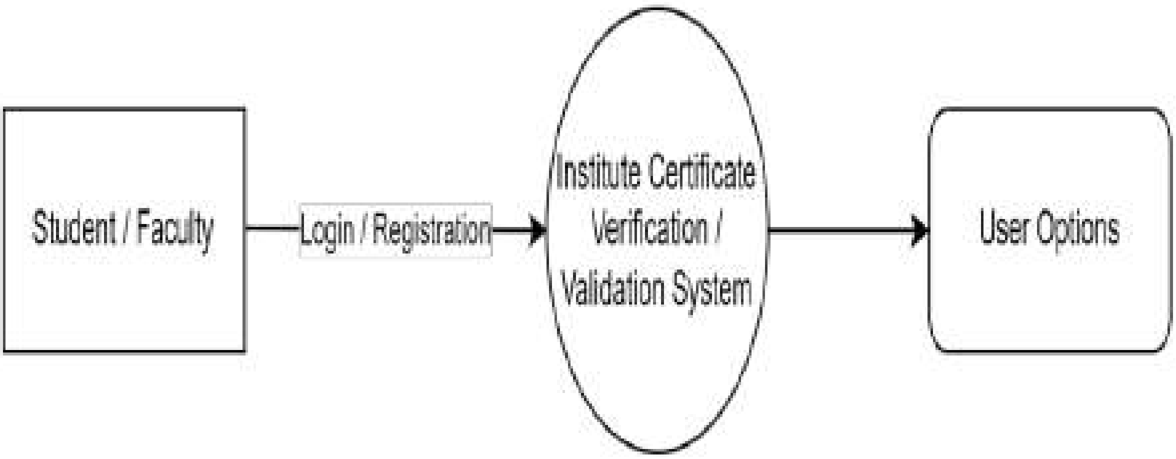


Figure 3.6: DFD Level 0

The login and registration feature in the system is designed to enable students and faculty to access their accounts. Once logged in, they are granted access to multiple user options. This includes the ability to view their certificates and verify their authenticity. Users may also be able to download their certificates or request new ones through the system. These options are meant to provide an efficient and effective means of managing user accounts and certificates.

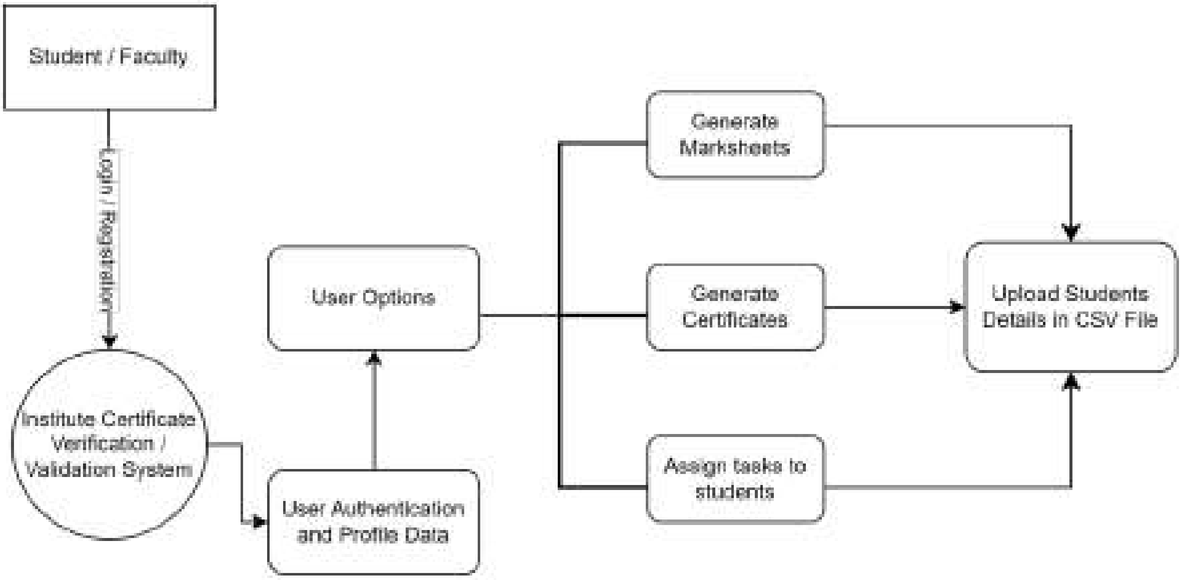

Student / Faculty
Login / Registration
Institute Certificate Verification / Validation System
User Authentication and Profile Data
User Options
Generate Marksheets
Generate Certificates
Assign tasks to students
Upload Students Details in CSV File

Figure 3.7: DFD Level 1

- Login/Registration: The process starts with users logging in or registering for the system.
- User Authentication and Profile Data: Once logged in, the system authenticates the user and retrieves their profile data. This data likely includes information relevant to the certification process, such as student ID or course enrollment details for students and faculty ID or course instruction details for faculty.
- User Options: After authentication, users are presented with options. These options include:

  1. Generate Marksheets: This suggests users can generate reports on their grades or performance.
  2. Upload Students Details in CSV File: This allows faculty (or authorized personnel) to upload student information in bulk, possibly for a new course or program.
  3. Generate Certificates: This is likely the core function, allowing users to generate certificates.
  4. Assign tasks to students: This block indicates faculty or administrators can assign tasks (possibly tests or assignments) to students through the system.

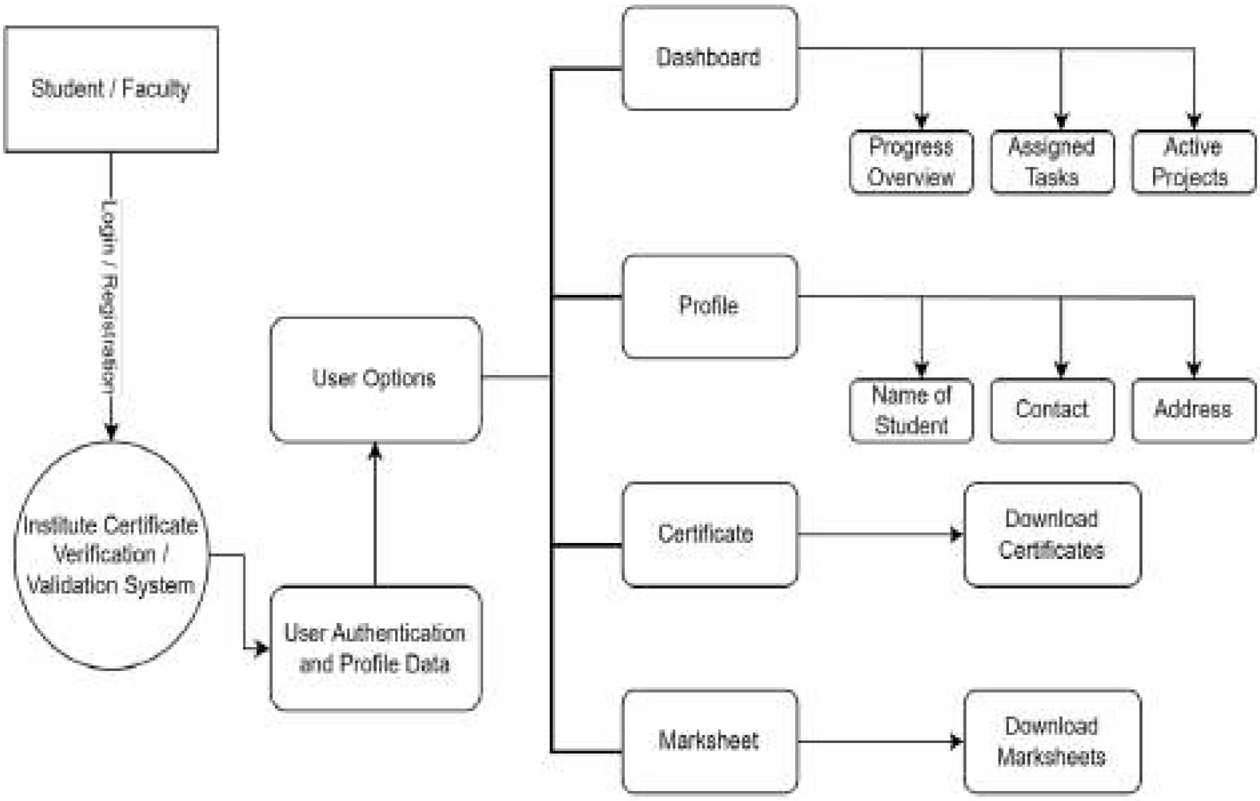


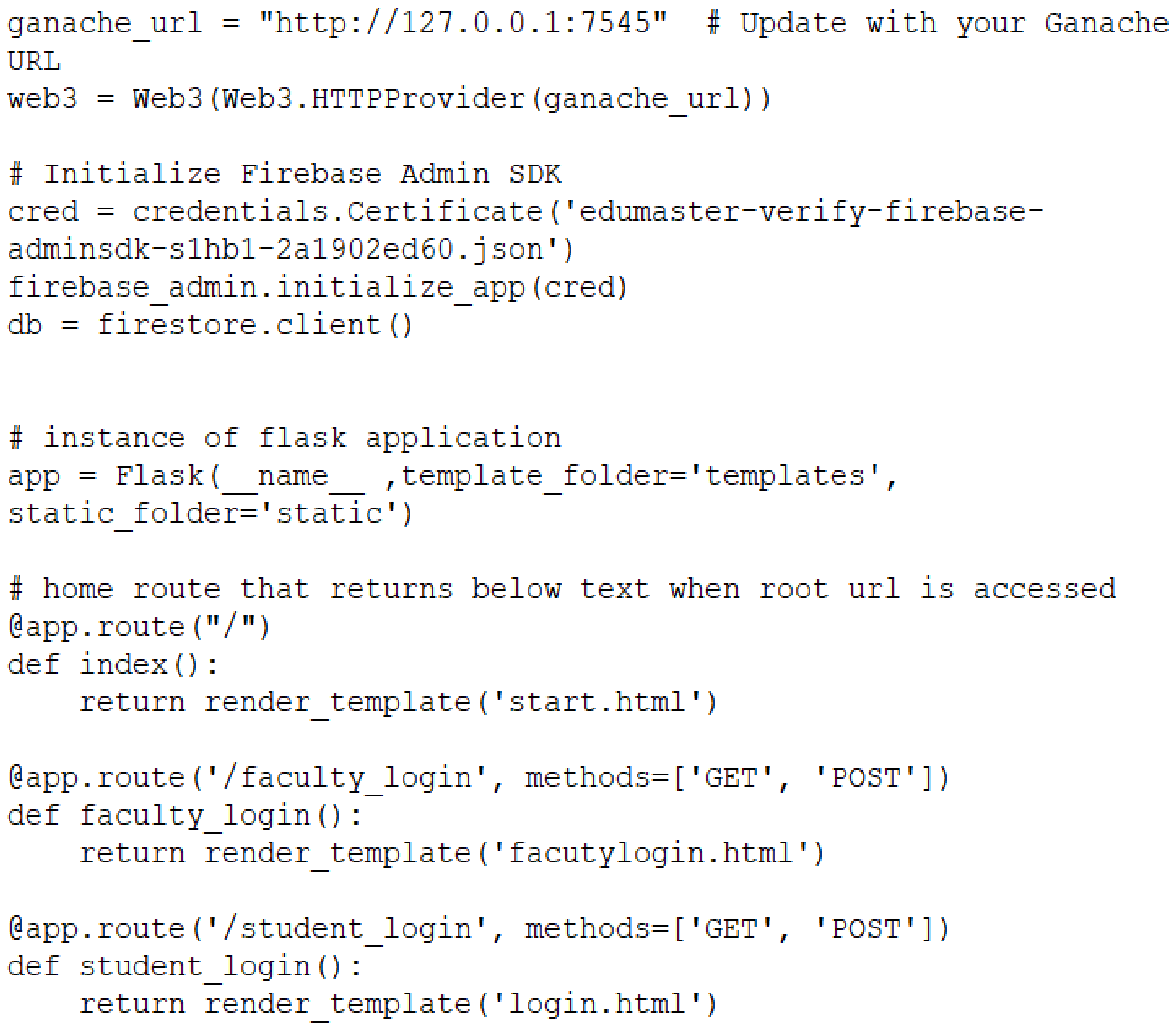
Figure 3.8: DFD Level 2

- Dashboard: The system revolves around a dashboard that provides an overview of student's academic records.
- Progress, Assigned, Active: These sections might be specific to students and could represent the progress of their coursework, assigned tasks, and active projects.
- Profile: This section likely allows students to access and update their profile information.
- Students: They can download certificates and access verification/validation options for their certificates.
- Faculty: They can't download certificates but have access to an "Institute Certificate Verification/Validation System". This suggests faculty can validate certificates issued by the institute, possibly for verification requests from employers or other institutions.
- Marksheets and Certificates: These sections allow students to download their marksheets and certificates.

Chapter 4

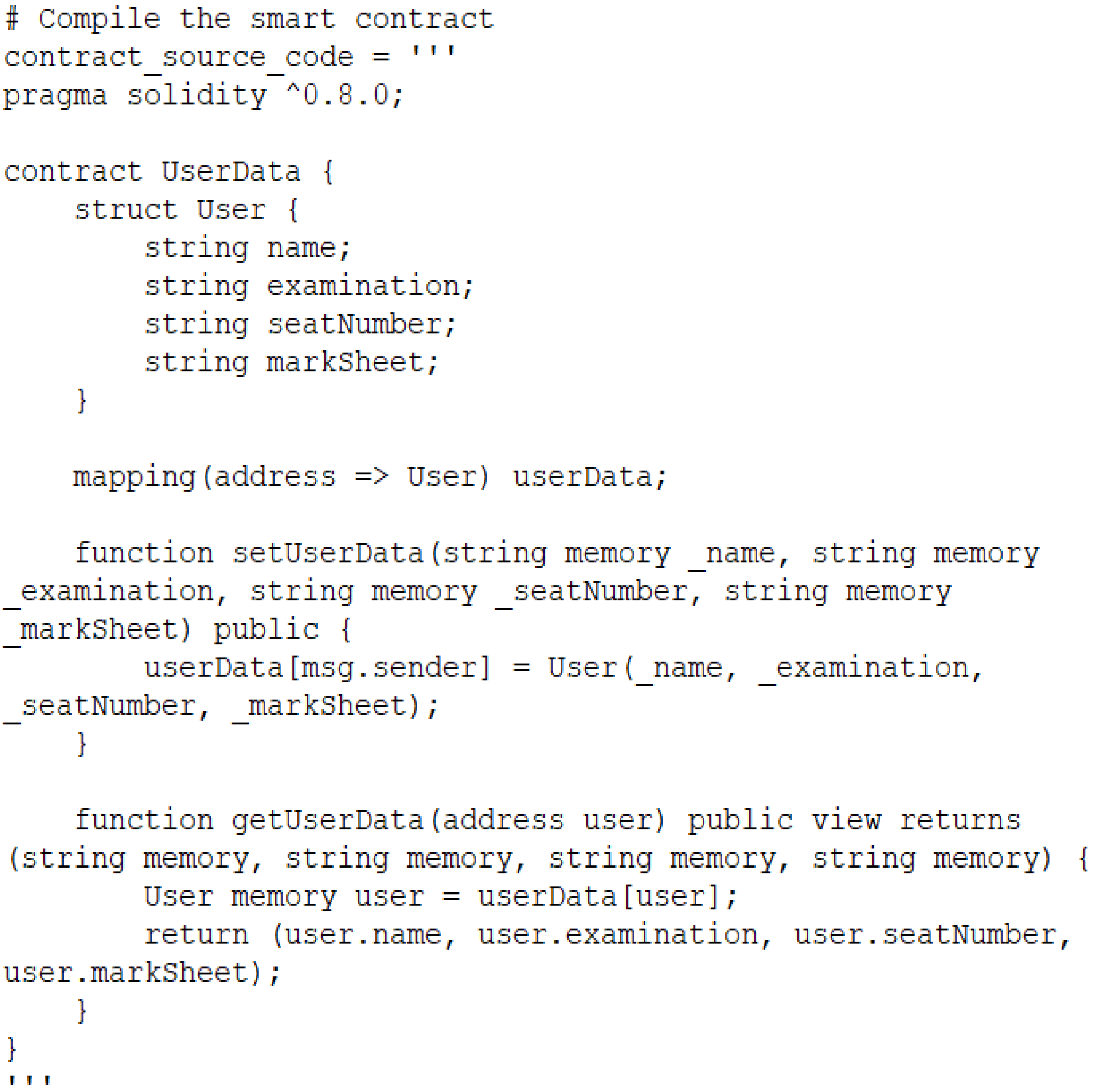
Project Implementation

4.1 Code Snippets



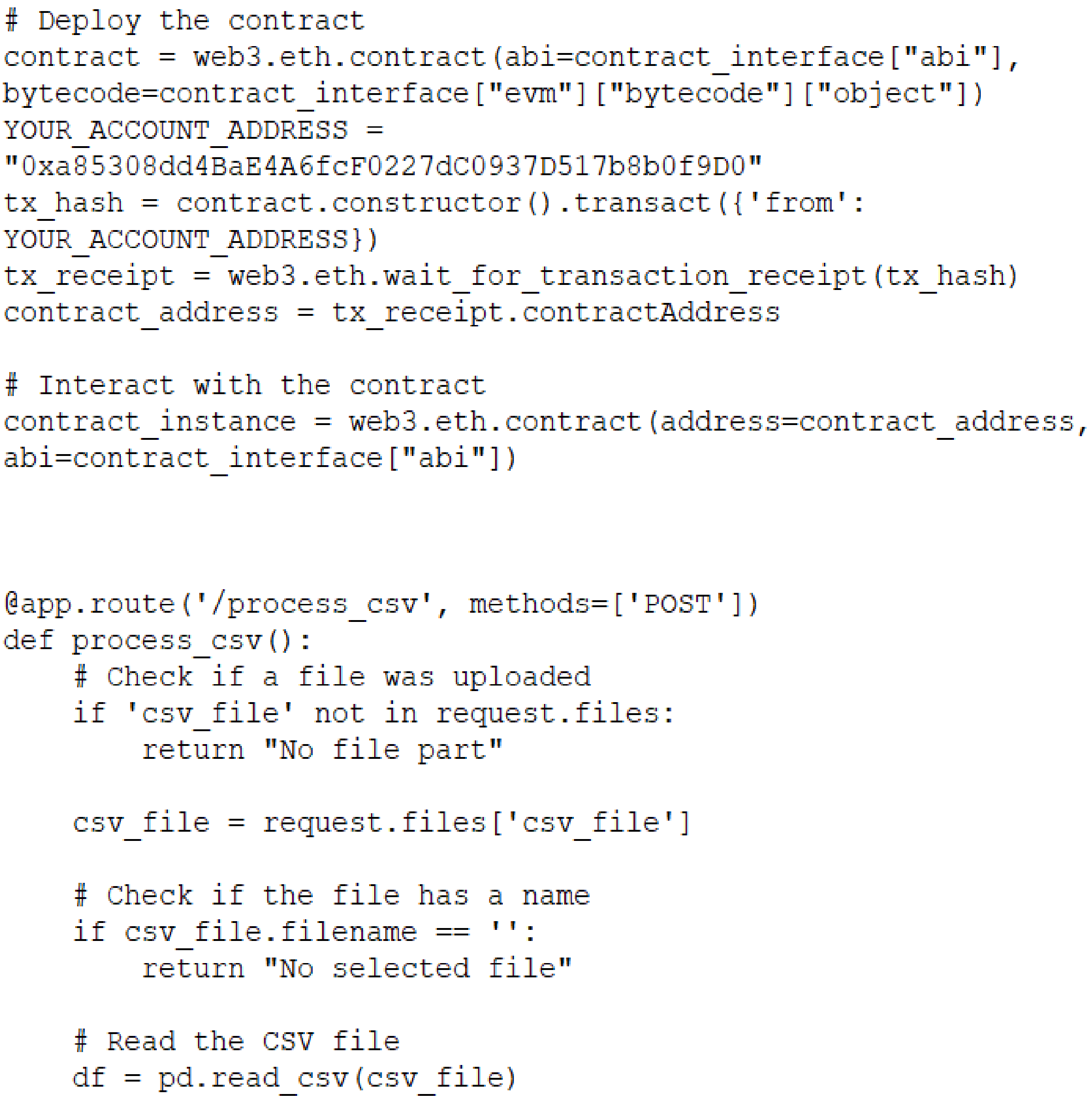
```
ganache_url = "http://127.0.0.1:7545"  # Update with your Ganache
URL
web3 = Web3(Web3.HTTPProvider(ganache_url))

# Initialize Firebase Admin SDK
cred = credentials.Certificate('edumaster-verify-firebase-
adminsdk-s1hb1-2a1902ed60.json')
firebase_admin.initialize_app(cred)
db = firestore.client()


# instance of flask application
app = Flask(__name__ ,template_folder='templates',
static_folder='static')

# home route that returns below text when root url is accessed
@app.route("/")
def index():
    return render_template('start.html')

@app.route('/faculty_login', methods=['GET', 'POST'])
def faculty_login():
    return render_template('facutylogin.html')

@app.route('/student_login', methods=['GET', 'POST'])
def student_login():
    return render_template('login.html')
```

Figure 4.1: Creating Flask Application



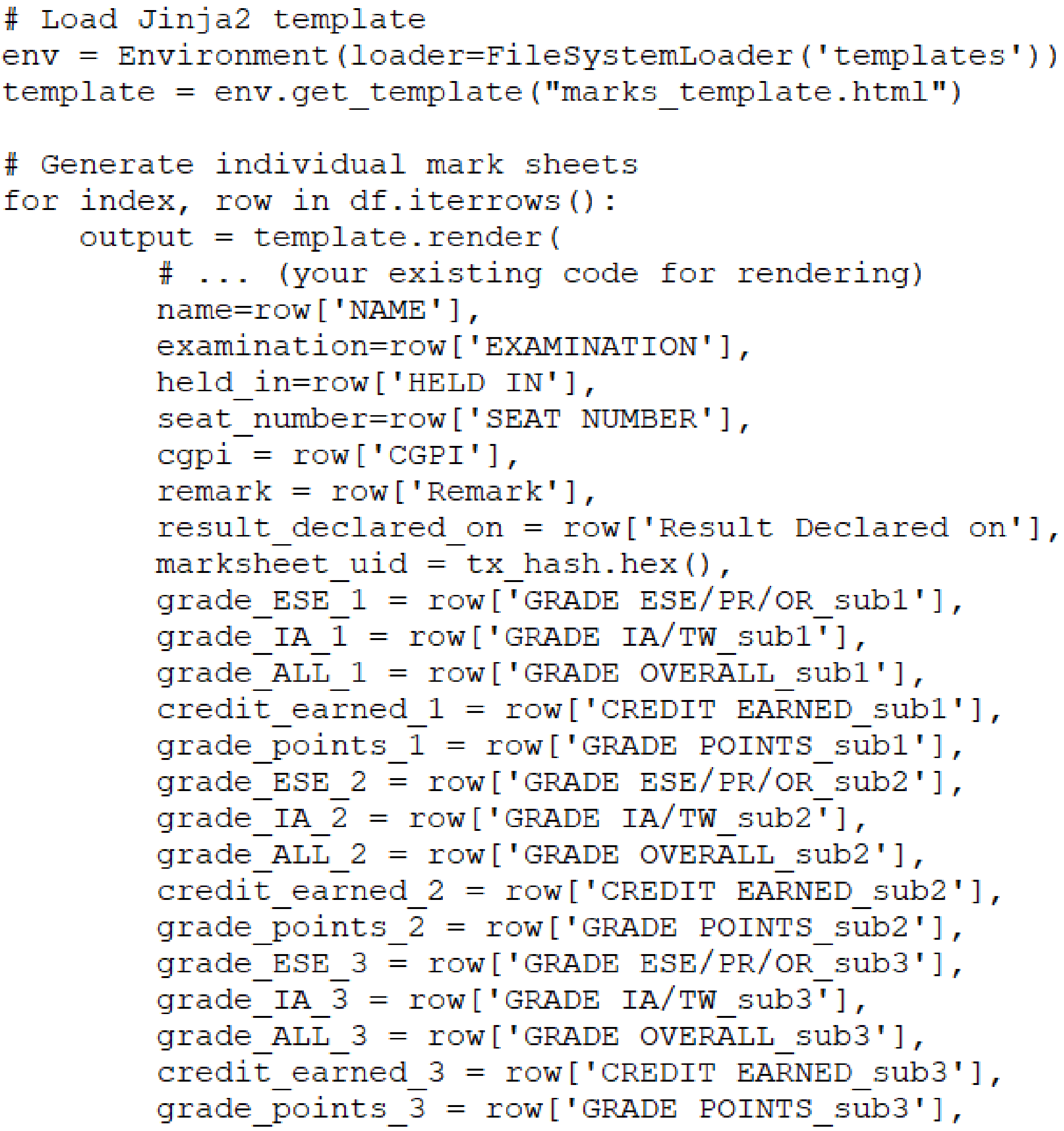
```
# Compile the smart contract
contract_source_code = '''
pragma solidity ^0.8.0;

contract UserData {
    struct User {
        string name;
        string examination;
        string seatNumber;
        string markSheet;
    }

    mapping(address => User) userData;

    function setUserData(string memory _name, string memory
_examination, string memory _seatNumber, string memory
_markSheet) public {
        userData[msg.sender] = User(_name, _examination,
_seatNumber, _markSheet);
    }

    function getUserData(address user) public view returns
(string memory, string memory, string memory, string memory) {
        User memory user = userData[user];
        return (user.name, user.examination, user.seatNumber,
user.markSheet);
    }
}
'''
```

Figure 4.2: Compile Smart Contract



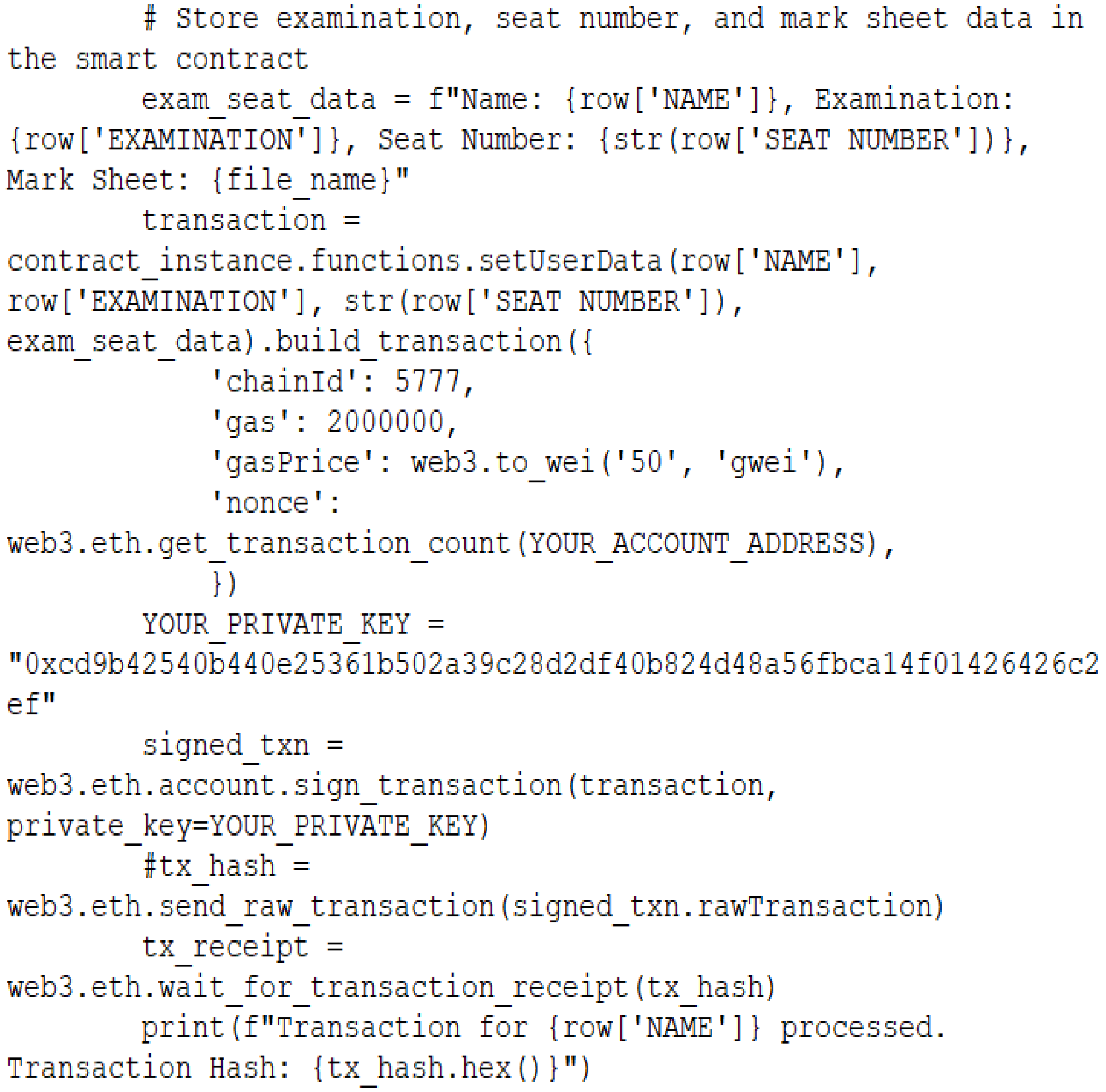
```
# Deploy the contract
contract = web3.eth.contract(abi=contract_interface["abi"],
bytecode=contract_interface["evm"]["bytecode"]["object"])
YOUR_ACCOUNT_ADDRESS =
"0xa85308dd4BaE4A6fcF0227dC0937D517b8b0f9D0"
tx_hash = contract.constructor().transact({'from':
YOUR_ACCOUNT_ADDRESS})
tx_receipt = web3.eth.wait_for_transaction_receipt(tx_hash)
contract_address = tx_receipt.contractAddress

# Interact with the contract
contract_instance = web3.eth.contract(address=contract_address,
abi=contract_interface["abi"])



@app.route('/process_csv', methods=['POST'])
def process_csv():
    # Check if a file was uploaded
    if 'csv_file' not in request.files:
        return "No file part"

    csv_file = request.files['csv_file']

    # Check if the file has a name
    if csv_file.filename == '':
        return "No selected file"

    # Read the CSV file
    df = pd.read_csv(csv_file)
```

Figure 4.3: Deploy Smart Contract



```
# Load Jinja2 template
env = Environment(loader=FileSystemLoader('templates'))
template = env.get_template("marks_template.html")

# Generate individual mark sheets
for index, row in df.iterrows():
    output = template.render(
        # ... (your existing code for rendering)
        name=row['NAME'],
        examination=row['EXAMINATION'],
        held_in=row['HELD IN'],
        seat_number=row['SEAT NUMBER'],
        cgpi = row['CGPI'],
        remark = row['Remark'],
        result_declared_on = row['Result Declared on'],
        marksheet_uid = tx_hash.hex(),
        grade_ESE_1 = row['GRADE ESE/PR/OR_sub1'],
        grade_IA_1 = row['GRADE IA/TW_sub1'],
        grade_ALL_1 = row['GRADE OVERALL_sub1'],
        credit_earned_1 = row['CREDIT EARNED_sub1'],
        grade_points_1 = row['GRADE POINTS_sub1'],
        grade_ESE_2 = row['GRADE ESE/PR/OR_sub2'],
        grade_IA_2 = row['GRADE IA/TW_sub2'],
        grade_ALL_2 = row['GRADE OVERALL_sub2'],
        credit_earned_2 = row['CREDIT EARNED_sub2'],
        grade_points_2 = row['GRADE POINTS_sub2'],
        grade_ESE_3 = row['GRADE ESE/PR/OR_sub3'],
        grade_IA_3 = row['GRADE IA/TW_sub3'],
        grade_ALL_3 = row['GRADE OVERALL_sub3'],
        credit_earned_3 = row['CREDIT EARNED_sub3'],
        grade_points_3 = row['GRADE POINTS_sub3'],
```

Figure 4.4: Define Templates Values



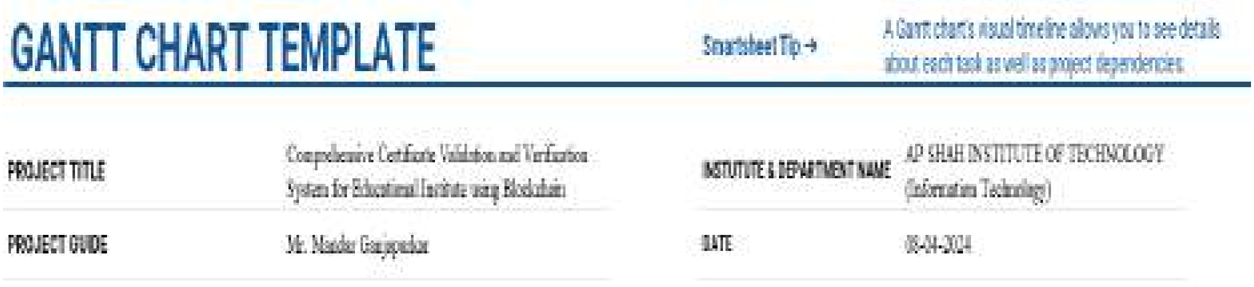
```
        # Store examination, seat number, and mark sheet data in
the smart contract
        exam_seat_data = f"Name: {row['NAME']}, Examination:
{row['EXAMINATION']}, Seat Number: {str(row['SEAT NUMBER'])},
Mark Sheet: {file_name}"
        transaction =
contract_instance.functions.setUserData(row['NAME'],
row['EXAMINATION'], str(row['SEAT NUMBER']),
exam_seat_data).build_transaction({
            'chainId': 5777,
            'gas': 2000000,
            'gasPrice': web3.to_wei('50', 'gwei'),
            'nonce':
web3.eth.get_transaction_count(YOUR_ACCOUNT_ADDRESS),
            })
        YOUR_PRIVATE_KEY =
"0xcd9b42540b440e25361b502a39c28d2df40b824d48a56fbca14f01426426c2
ef"
        signed_txn =
web3.eth.account.sign_transaction(transaction,
private_key=YOUR_PRIVATE_KEY)
        #tx_hash =
web3.eth.send_raw_transaction(signed_txn.rawTransaction)
        tx_receipt =
web3.eth.wait_for_transaction_receipt(tx_hash)
        print(f"Transaction for {row['NAME']} processed.
Transaction Hash: {tx_hash.hex()}")
```

Figure 4.5: Transaction Process

4.2 Steps to access the System

1. The system involves three different user sides, namely Educator, Student, and Verifier.
2. All user sides are connected through web applications that are developed using modern web technologies such as HTML 5, CSS 3, Bootstrap, and JavaScript.
3. The users interact with the Ethereum Blockchain through the internet, which is hosted on a server that interacts with a database for storing user details and generated documents.
4. The system is designed to enable Educators to create and issue certificates, students to receive and access certificates, and verifiers to verify and validate certificates.
5. The system leverages smart contracts to implement the logic and rules for creating, issuing, verifying, validating, revoking, and renewing certificates.
6. The database stores user details and generated documents, such as certificates, QR codes, and verification results.
7. You can easily access and download your certificates and marksheets, and view the tasks assigned to you, as well as the ongoing projects you're involved in.
8. You can track your progress and stay updated on your academic achievements.
9. With this system, faculty members can generate certificates and marksheets with ease and accuracy.
10. In addition, the system allows faculty members to assign specific tasks to individual students, ensuring that all requirements are met for the successful completion of the certification process.
11. It not only ensures the authenticity of a student's mark sheet or certificate but also provides access to external entities such as universities or institutes for verification purposes.
12. This is achieved through the use of a QR code that is printed on the document or a unique ID that is assigned to the mark sheet or certificate.
13. By using this system, external entities can easily and accurately verify the validity of a student's credentials.

4.3 Timeline Sem VIII

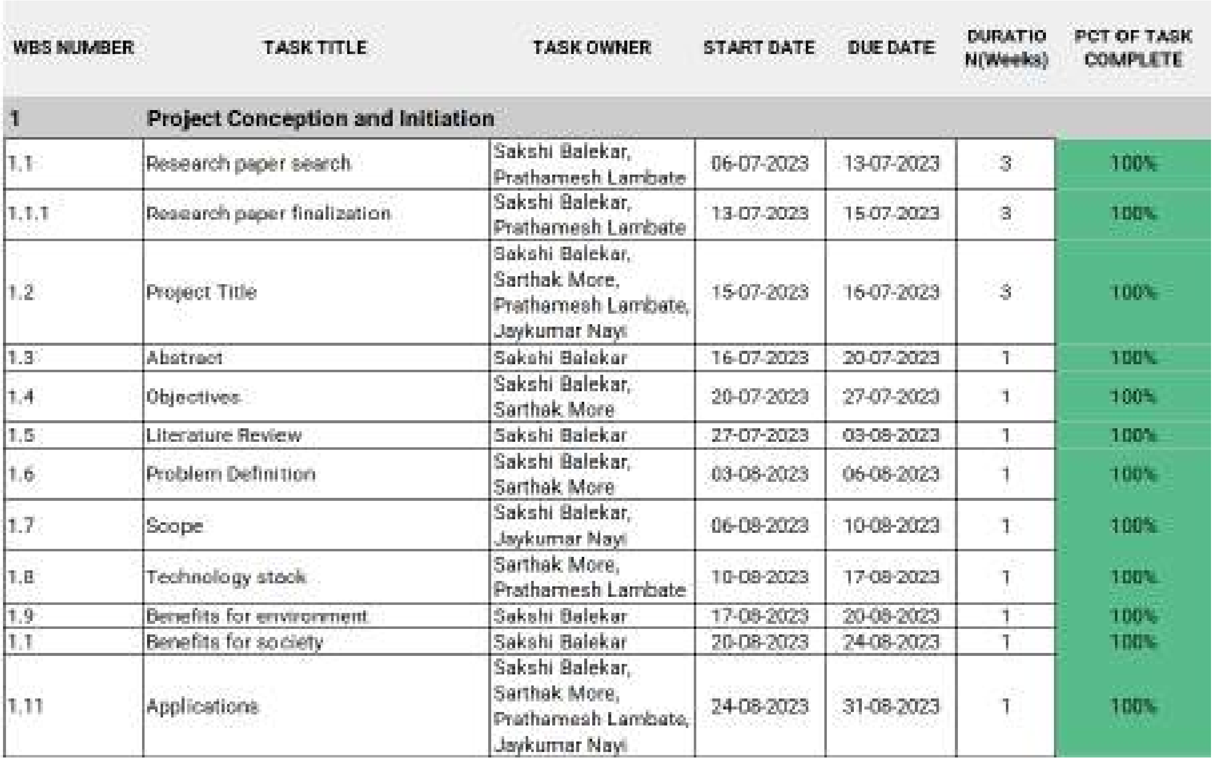


GANTT CHART TEMPLATE

Smartsheet Tip → A Gantt chart's visual timeline allows you to see details about each task as well as project dependencies.

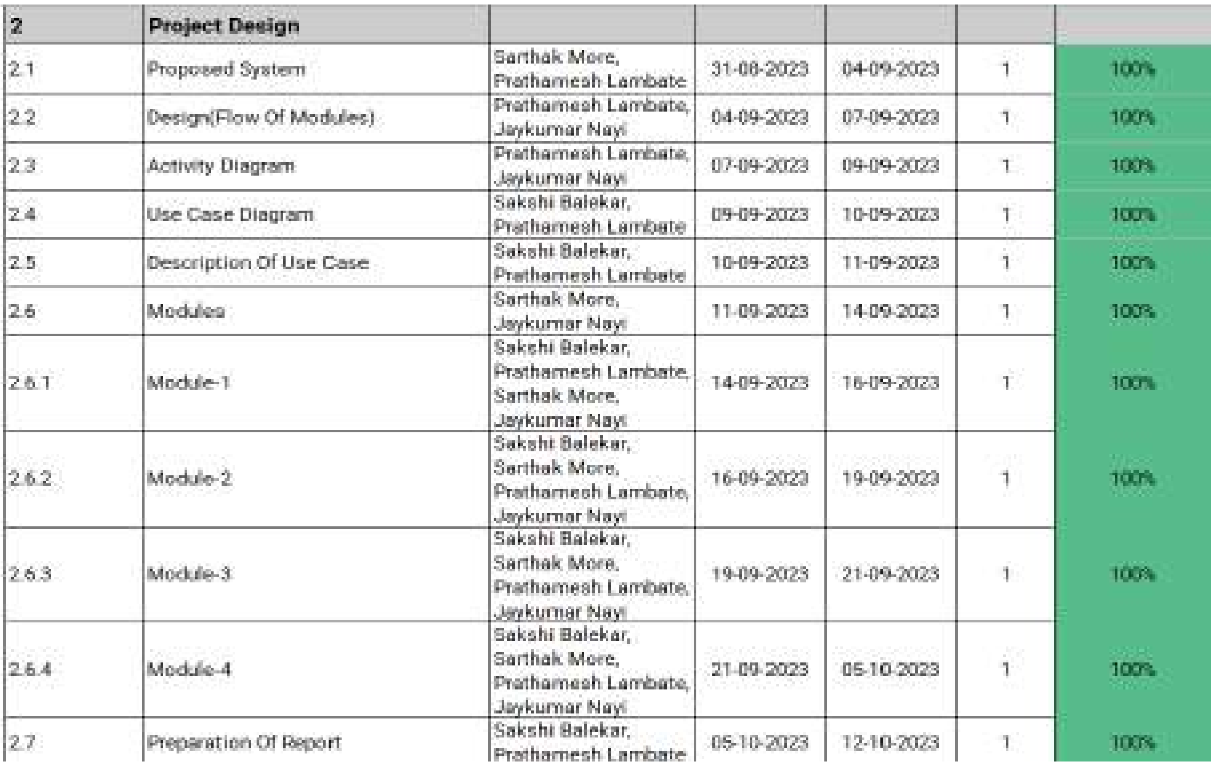
PROJECT TITLE	Comprehensive Certificate Validation and Verification System for Educational Institute using Blockchain	INSTITUTE & DEPARTMENT NAME	AP SHAH INSTITUTE OF TECHNOLOGY (Information Technology)
PROJECT GUIDE	Mr. Mandar Ganjapurkar	DATE	08-04-2024

Figure 4.6: Ganntt Chart 01



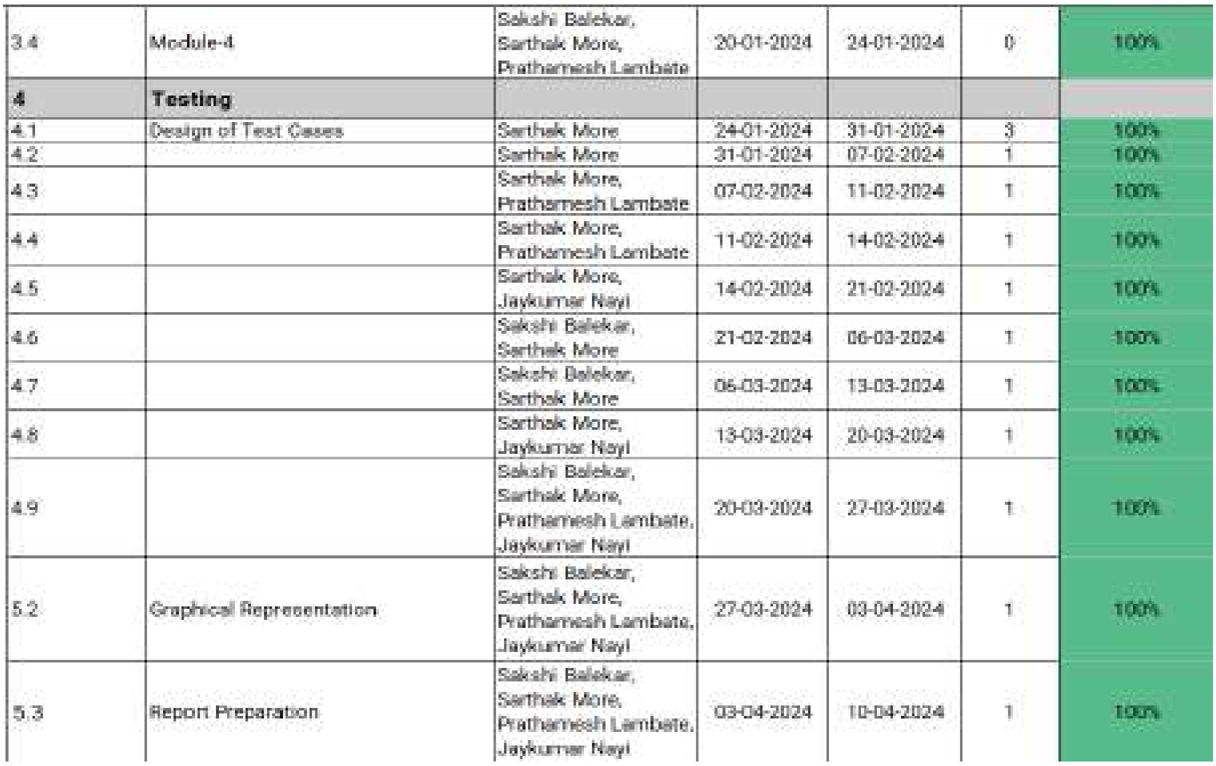
WBS NUMBER	TASK TITLE	TASK OWNER	START DATE	DUE DATE	DURATIO N(Weeks)	PCT OF TASK COMPLETE
1	Project Conception and Initiation					
1.1	Research paper search	Sakshi Balekar, Prathamesh Lambate	06-07-2023	13-07-2023	3	100%
1.1.1	Research paper finalization	Sakshi Balekar, Prathamesh Lambate	13-07-2023	15-07-2023	3	100%
1.2	Project Title	Sakshi Balekar, Sarthak More, Prathamesh Lambate, Jaykumar Nayi	15-07-2023	16-07-2023	3	100%
1.3	Abstract	Sakshi Balekar	16-07-2023	20-07-2023	1	100%
1.4	Objectives	Sakshi Balekar, Sarthak More	20-07-2023	27-07-2023	1	100%
1.5	Literature Review	Sakshi Balekar	27-07-2023	03-08-2023	1	100%
1.6	Problem Definition	Sakshi Balekar, Sarthak More	03-08-2023	06-08-2023	1	100%
1.7	Scope	Sakshi Balekar, Jaykumar Nayi	06-08-2023	10-08-2023	1	100%
1.8	Technology stack	Sarthak More, Prathamesh Lambate	10-08-2023	17-08-2023	1	100%
1.9	Benefits for environment	Sakshi Balekar	17-08-2023	20-08-2023	1	100%
1.1	Benefits for society	Sakshi Balekar	20-08-2023	24-08-2023	1	100%
1.11	Applications	Sakshi Balekar, Sarthak More, Prathamesh Lambate, Jaykumar Nayi	24-08-2023	31-08-2023	1	100%

Figure 4.7: Ganntt Chart 02



2	**Project Design**					
2.1	Proposed System	Sarthak More, Prathamesh Lambate	31-08-2023	04-09-2023	1	100%
2.2	Design(Flow Of Modules)	Prathamesh Lambate, Jaykumar Nayi	04-09-2023	07-09-2023	1	100%
2.3	Activity Diagram	Prathamesh Lambate, Jaykumar Nayi	07-09-2023	09-09-2023	1	100%
2.4	Use Case Diagram	Sakshi Balekar, Prathamesh Lambate	09-09-2023	10-09-2023	1	100%
2.5	Description Of Use Case	Sakshi Balekar, Prathamesh Lambate	10-09-2023	11-09-2023	1	100%
2.6	Modules	Sarthak More, Jaykumar Nayi	11-09-2023	14-09-2023	1	100%
2.6.1	Module-1	Sakshi Balekar, Prathamesh Lambate, Sarthak More, Jaykumar Nayi	14-09-2023	16-09-2023	1	100%
2.6.2	Module-2	Sakshi Balekar, Sarthak More, Prathamesh Lambate, Jaykumar Nayi	16-09-2023	19-09-2023	1	100%
2.6.3	Module-3	Sakshi Balekar, Sarthak More, Prathamesh Lambate, Jaykumar Nayi	19-09-2023	21-09-2023	1	100%
2.6.4	Module-4	Sakshi Balekar, Sarthak More, Prathamesh Lambate, Jaykumar Nayi	21-09-2023	05-10-2023	1	100%
2.7	Preparation Of Report	Sakshi Balekar, Prathamesh Lambate	05-10-2023	12-10-2023	1	100%

Figure 4.8: Ganntt Chart 03



3.4	Module-4	Sakshi Balekar, Sarthak More, Prathamesh Lambate	20-01-2024	24-01-2024	0	100%
4	**Testing**					
4.1	Design of Test Cases	Sarthak More	24-01-2024	31-01-2024	3	100%
4.2		Sarthak More	31-01-2024	07-02-2024	1	100%
4.3		Sarthak More, Prathamesh Lambate	07-02-2024	11-02-2024	1	100%
4.4		Sarthak More, Prathamesh Lambate	11-02-2024	14-02-2024	1	100%
4.5		Sarthak More, Jaykumar Nayi	14-02-2024	21-02-2024	1	100%
4.6		Sakshi Balekar, Sarthak More	21-02-2024	06-03-2024	1	100%
4.7		Sakshi Balekar, Sarthak More	06-03-2024	13-03-2024	1	100%
4.8		Sarthak More, Jaykumar Nayi	13-03-2024	20-03-2024	1	100%
4.9		Sakshi Balekar, Sarthak More, Prathamesh Lambate, Jaykumar Nayi	20-03-2024	27-03-2024	1	100%
5.2	Graphical Representation	Sakshi Balekar, Sarthak More, Prathamesh Lambate, Jaykumar Nayi	27-03-2024	03-04-2024	1	100%
5.3	Report Preparation	Sakshi Balekar, Sarthak More, Prathamesh Lambate, Jaykumar Nayi	03-04-2024	10-04-2024	1	100%

Figure 4.9: Ganntt Chart 04

Chapter 5

Testing

5.1 Software Testing

Software testing is a process of evaluating a software product to ensure that it meets the specified requirements and works correctly. The main goal of software testing is to identify defects or errors in the software and to ensure that the software meets the business and technical requirements, is reliable, and performs as expected. The testing process includes a series of activities that can be performed manually or using automated tools, and it typically involves testing the functionality, performance, security, usability, and compatibility of the software. The ultimate goal of software testing is to improve the quality of the software and to ensure that it meets the needs and expectations of the users.

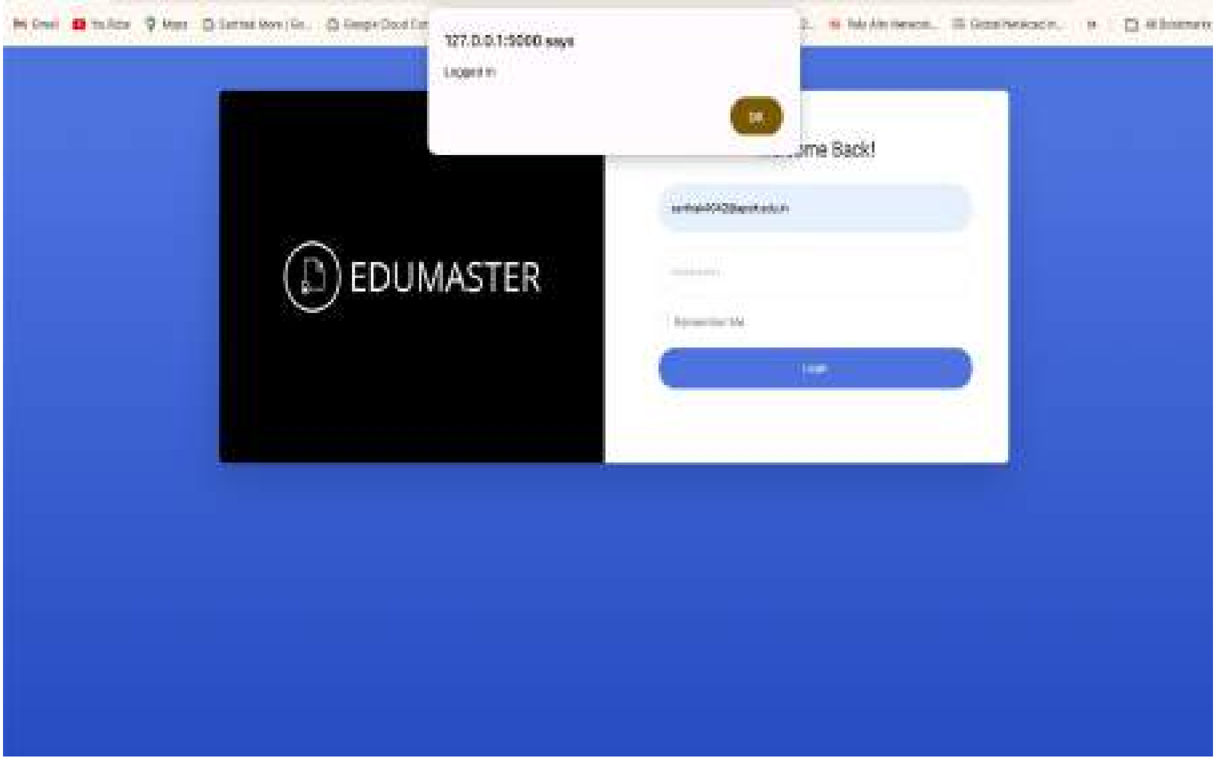
5.2 Functional Testing

Integration testing is a software testing technique that verifies the interfaces between software components or modules work correctly when integrated. This type of testing is performed after unit testing and before system testing to ensure that different software components work together as expected and that the system as a whole functions correctly. The purpose of integration testing is to identify any issues or defects that may arise from the interaction between the integrated components.

In this type of testing, individual units of code are combined and tested as a group to ensure they work together seamlessly. One of the main benefits of integration testing is that it helps to detect defects early on in the development process, which reduces the cost of fixing these issues later on. By performing integration testing, developers can identify and fix any issues before the system is released to the end-users. Overall, integration testing is an essential part of the software testing process that helps to ensure the quality and reliability of the software system.

Test case No.	Test case	Status of Test case
01	Login and Signup	Successful
02	Generate and authenticate certificates	Successful
03	Verify certificates stored in blockchain	Successful
04	Validate certificates stored in blockchain	Successful
05	External verifier verify certificates	Successful

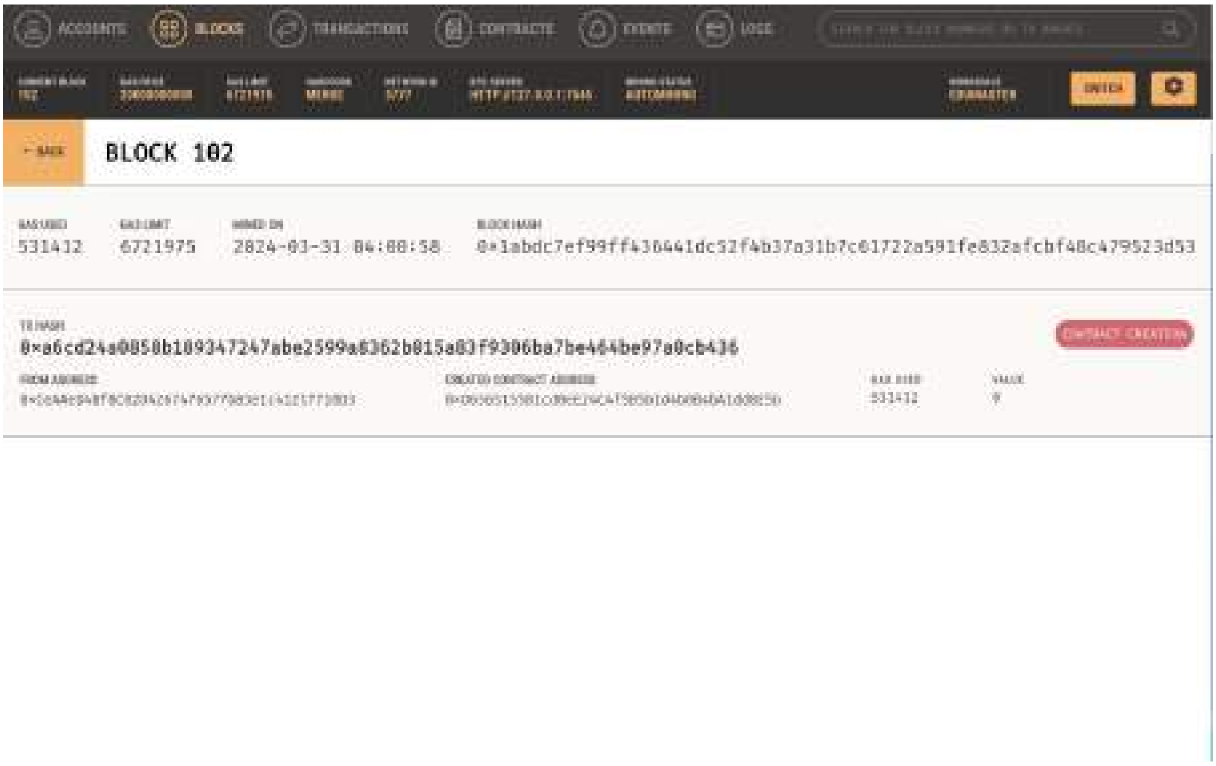
Table 5.1: Functional Testing



127.0.0.1:5000 says

Logged in

Figure 5.1: Test Case 01 (Login & signup)



CURRENT BLOCK 102 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE [illegible]

← BACK

BLOCK 102

GAS USED 531412

GAS LIMIT 6721975

MINED ON 2024-03-31 04:08:58

BLOCK HASH 0×1abdc7ef99ff436441dc52f4b37a31b7c61722a591fe832afcbf48c479523d53

TX HASH 0×a6cd24a0858b189347247abe2599a8362b015a83f9306ba7be464be97a0cb436

CONTRACT CREATION

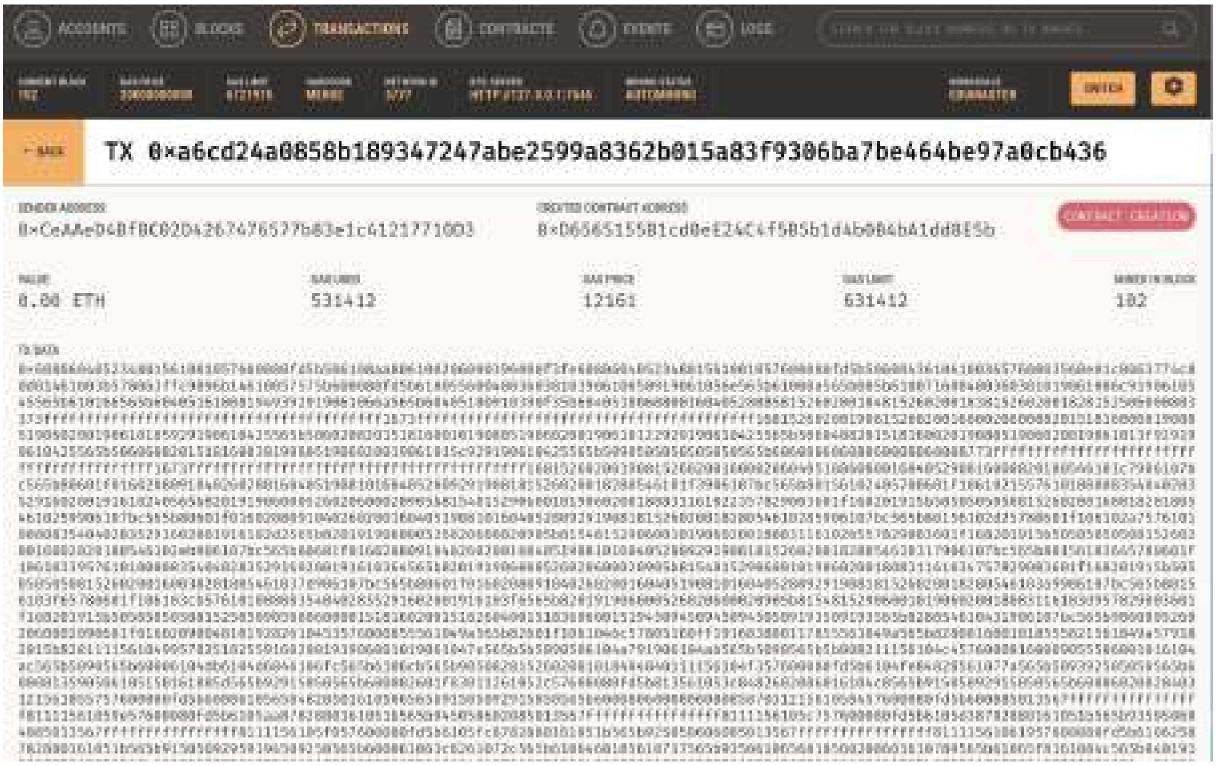
FROM ADDRESS 0×CeAAeD4BfBC02D4267476577b83e1c41217710D3

CREATED CONTRACT ADDRESS 0×D6565155B1cd0eE24C4f585b1d4b0B4bA1dd8E5b

GAS USED 531412

VALUE 0

Figure 5.2: Test Case 02 (Certificate Generation)



CURRENT BLOCK 102 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE [illegible]

← BACK

TX 0×a6cd24a0858b189347247abe2599a8362b015a83f9306ba7be464be97a0cb436

SENDER ADDRESS 0×CeAAeD4BfBC02D4267476577b83e1c41217710D3

CREATED CONTRACT ADDRESS 0×D6565155B1cd0eE24C4f585b1d4b0B4bA1dd8E5b

CONTRACT CREATION

VALUE 0.00 ETH

GAS USED 531412

GAS PRICE 12161

GAS LIMIT 631412

MINED IN BLOCK 102

TX DATA

```
[illegible]
```

Figure 5.3: Test Case 03 (Verify Certificates)

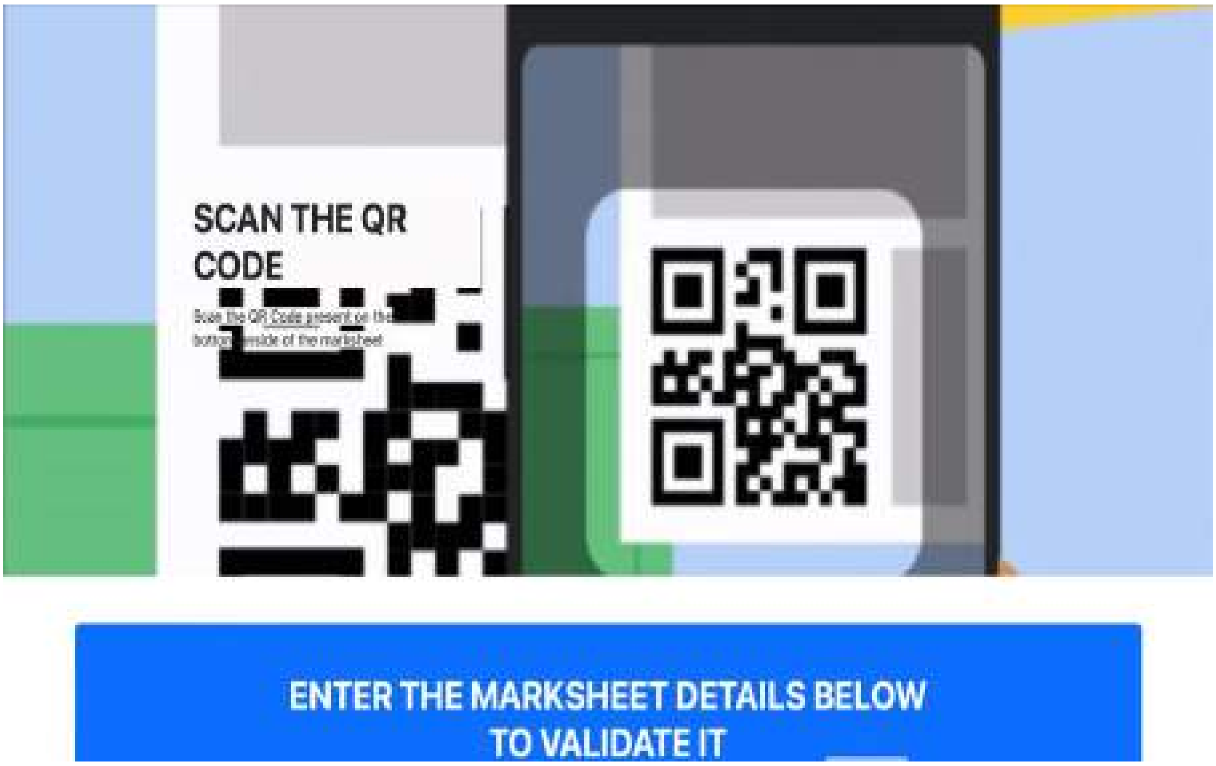
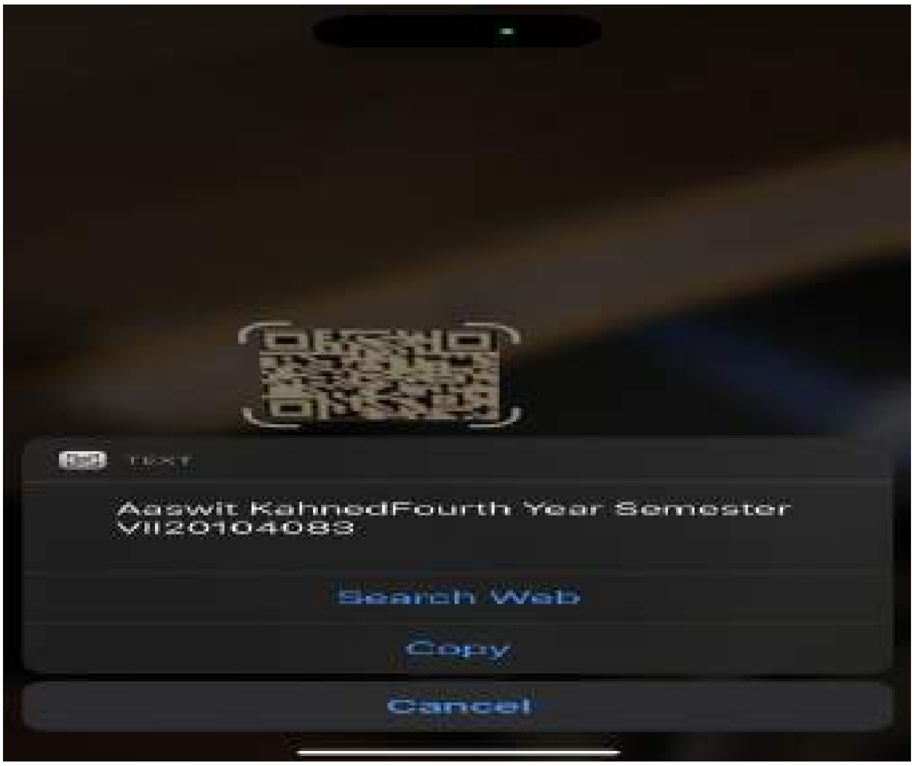
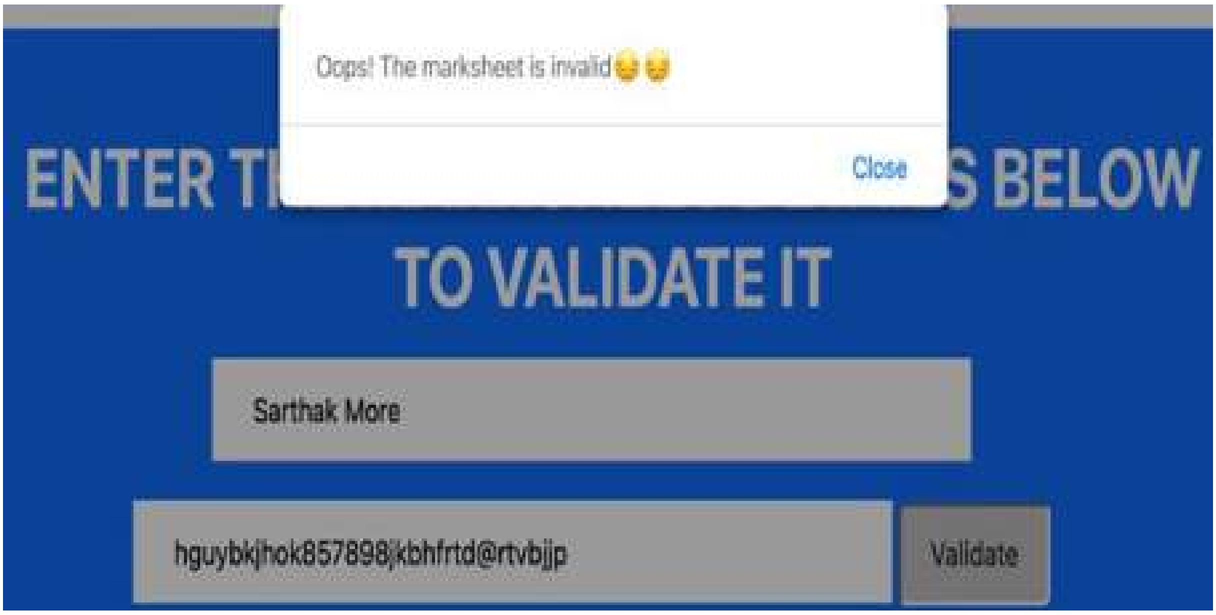

SCAN THE QR CODE
Scan the QR Code present on the bottom side of the marksheet
ENTER THE MARKSHEET DETAILS BELOW TO VALIDATE IT

Figure 5.4: Test Case 04 (Validating Certificates)



Aaswit KahnedFourth Year Semester VII201040 83

Figure 5.5: Test Case 05 (External verifier verify certificates)



Oops! The marksheet is invalid😔😔

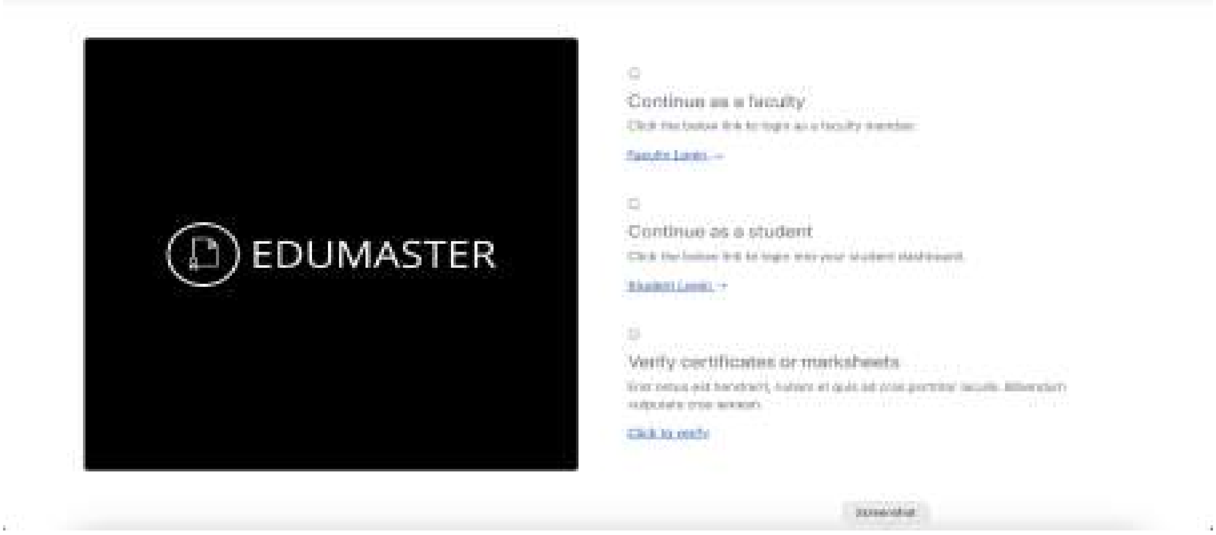
Sarthak More

hguybkjhok857898jkbhfrtd@rtvbjjp

Figure 5.6: Certificate Verification Unsuccessful

Chapter 6

Result and Discussions



Continue as a faculty

Click the below link to login as a faculty member.

Faculty Login →

Continue as a student

Click the below link to login into your student dashboard.

Student Login →

Verify certificates or marksheets

[illegible]

Click to verify

Figure 6.1: Login Page

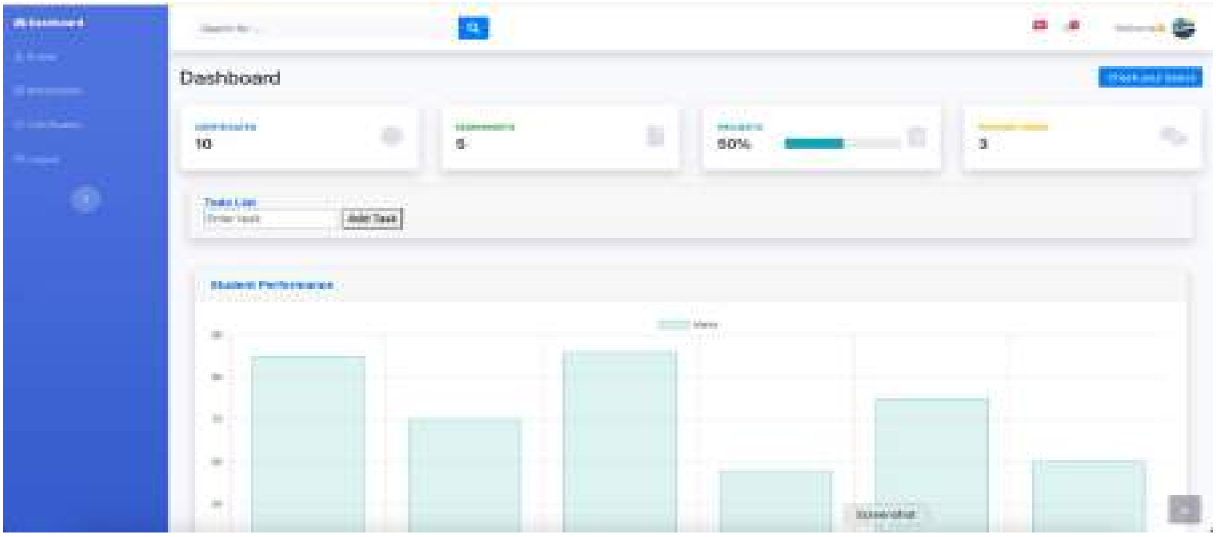
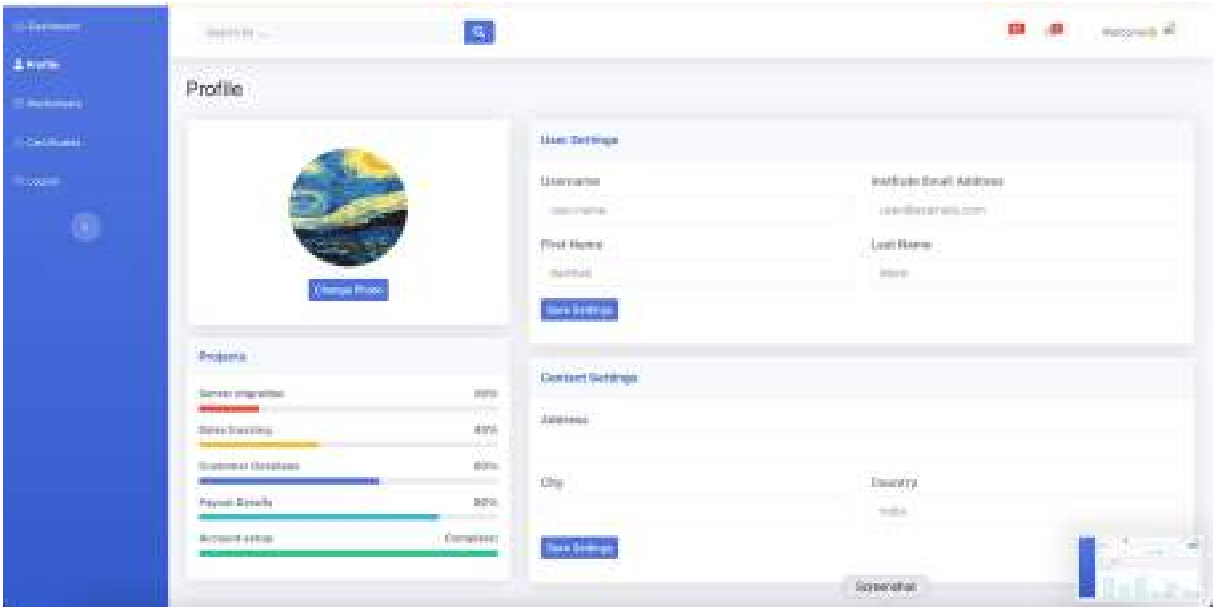


Figure 6.2: Student Dashboard Page



Profile

User Settings

Username: username

Institute Email Address: user@example.com

First Name

Last Name

Projects

Server migration	20%
Sales tracking	40%
Customer Database	60%
Payout Details	80%
Account setup	Complete!

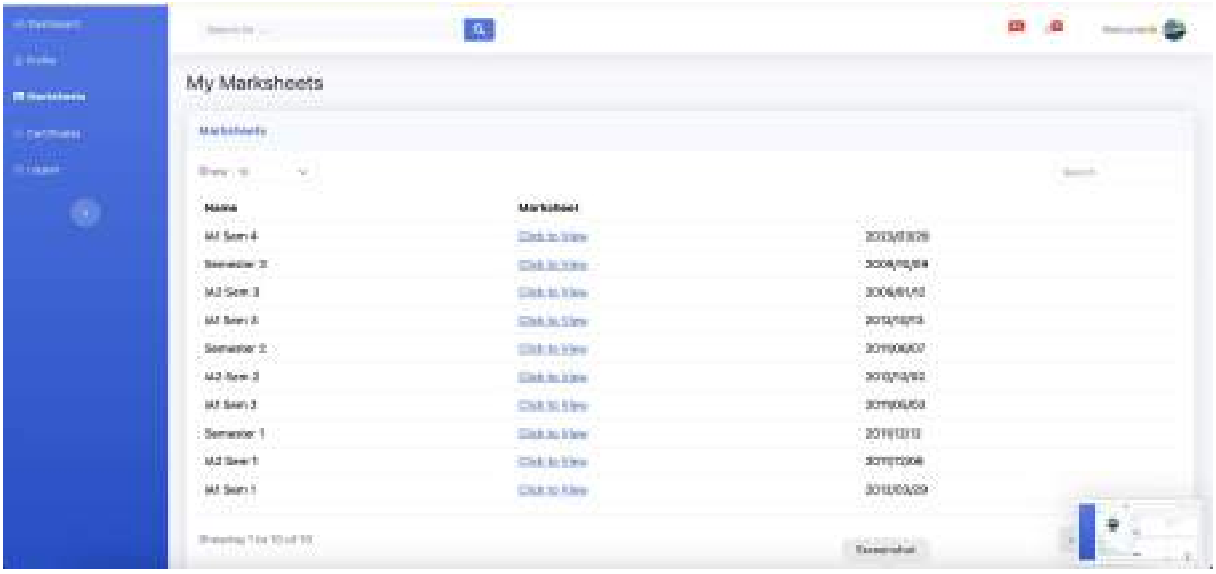
Contact Settings

Address

City

Country: India

Figure 6.3: Student Profile Page



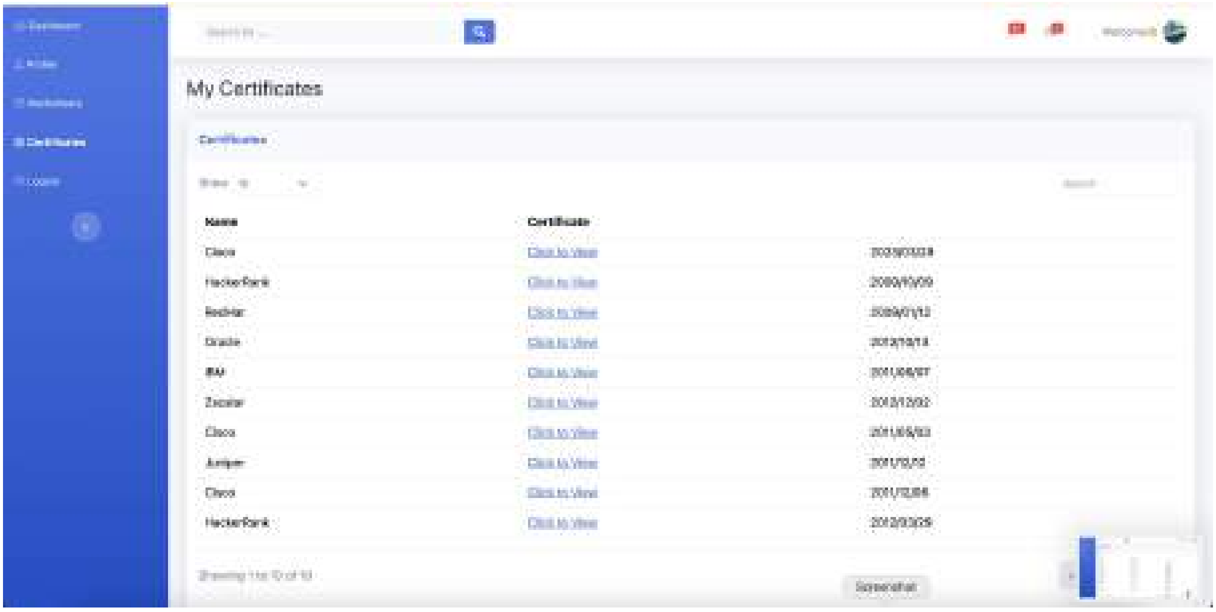
My Marksheets

Marksheets

Name	Marksheet	
IA1 Sem 4	Click to View	2023/03/29
Semester 3	Click to View	2009/10/09
IA2 Sem 3	Click to View	2009/01/12
IA1 Sem 3	Click to View	2012/10/13
Semester 2	Click to View	2011/06/07
IA2 Sem 2	Click to View	2012/12/02
IA1 Sem 2	Click to View	2011/05/03
Semester 1	Click to View	2011/12/12
IA2 Sem 1	Click to View	2011/12/06
IA1 Sem 1	Click to View	2012/03/29

Showing 1 to 10 of 10

Figure 6.4: Student Marksheets Page



My Certificates

Certificates

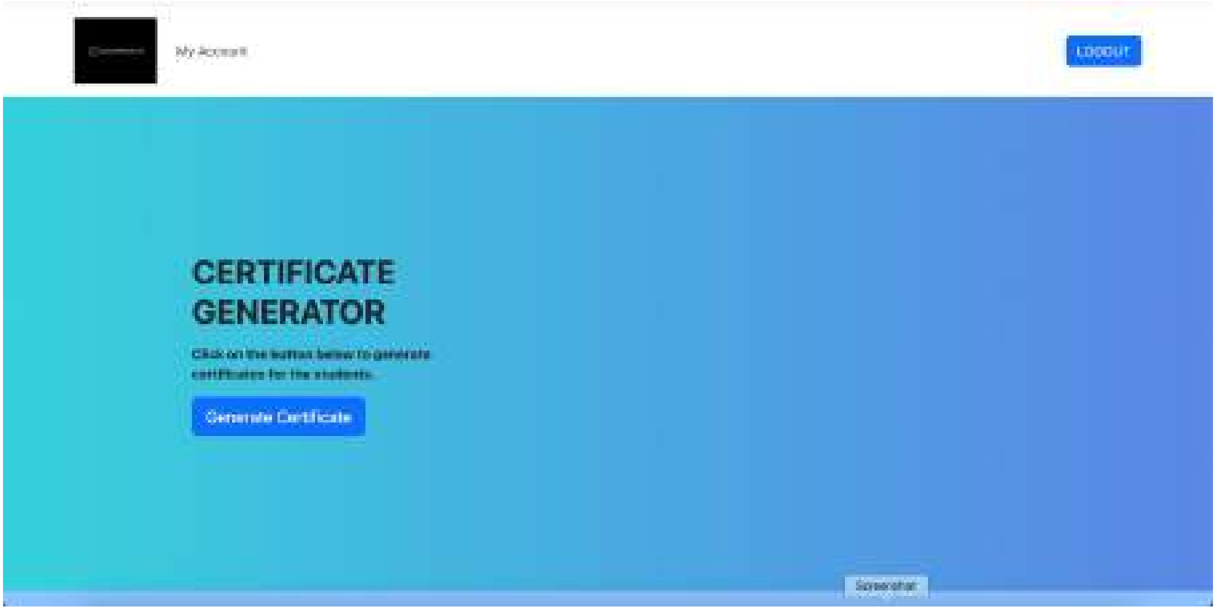
Show 10

Search:

Name	Certificate	
Cisco	Click to View	2023/03/28
HackerRank	Click to View	2020/10/09
Redhat	Click to View	2009/01/12
Oracle	Click to View	2012/10/14
IBM	Click to View	2011/06/07
Zscaler	Click to View	2012/12/02
Cisco	Click to View	2011/05/03
Juniper	Click to View	2011/12/12
Cisco	Click to View	2011/12/06
HackerRank	Click to View	2012/03/29

Showing 1 to 10 of 10

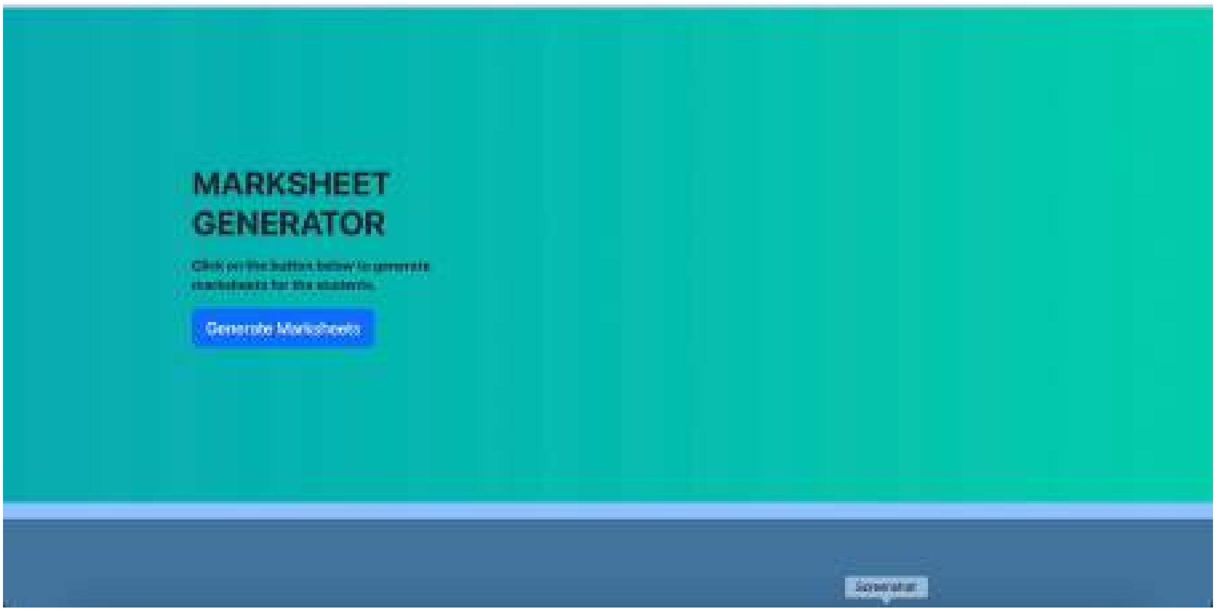
Figure 6.5: Student Certificates Page



CERTIFICATE GENERATOR

Click on the button below to generate certificates for the students.

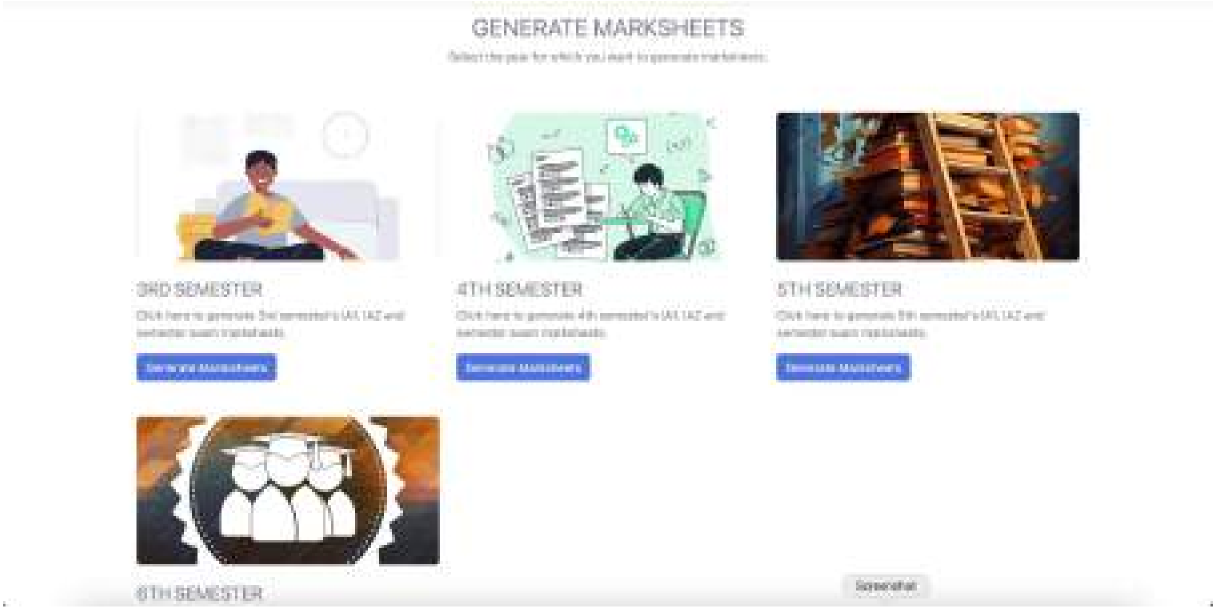
Figure 6.6: Certificate Generation Page



MARKSHEET GENERATOR

Click on the button below to generate marksheets for the students.

Figure 6.7: Marksheet Generation Page



GENERATE MARKSHEETS

Select the year for which you want to generate marksheets.

3RD SEMESTER

Click here to generate 3rd semester's IA1, IA2 and semester exam marksheets.

4TH SEMESTER

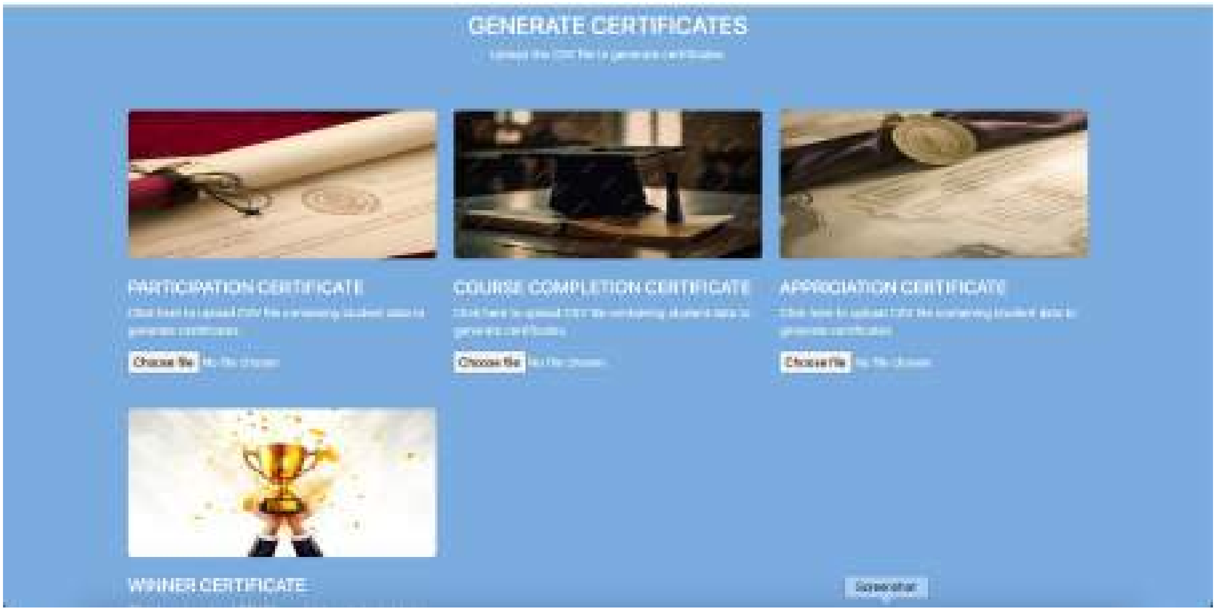
Click here to generate 4th semester's IA1, IA2 and semester exam marksheets.

5TH SEMESTER

Click here to generate 5th semester's IA1, IA2 and semester exam marksheets.

6TH SEMESTER

Figure 6.8: Generate Marksheet



GENERATE CERTIFICATES

Upload the CSV file to generate certificates

PARTICIPATION CERTIFICATE

Click here to upload CSV file containing student data to generate certificates

COURSE COMPLETION CERTIFICATE

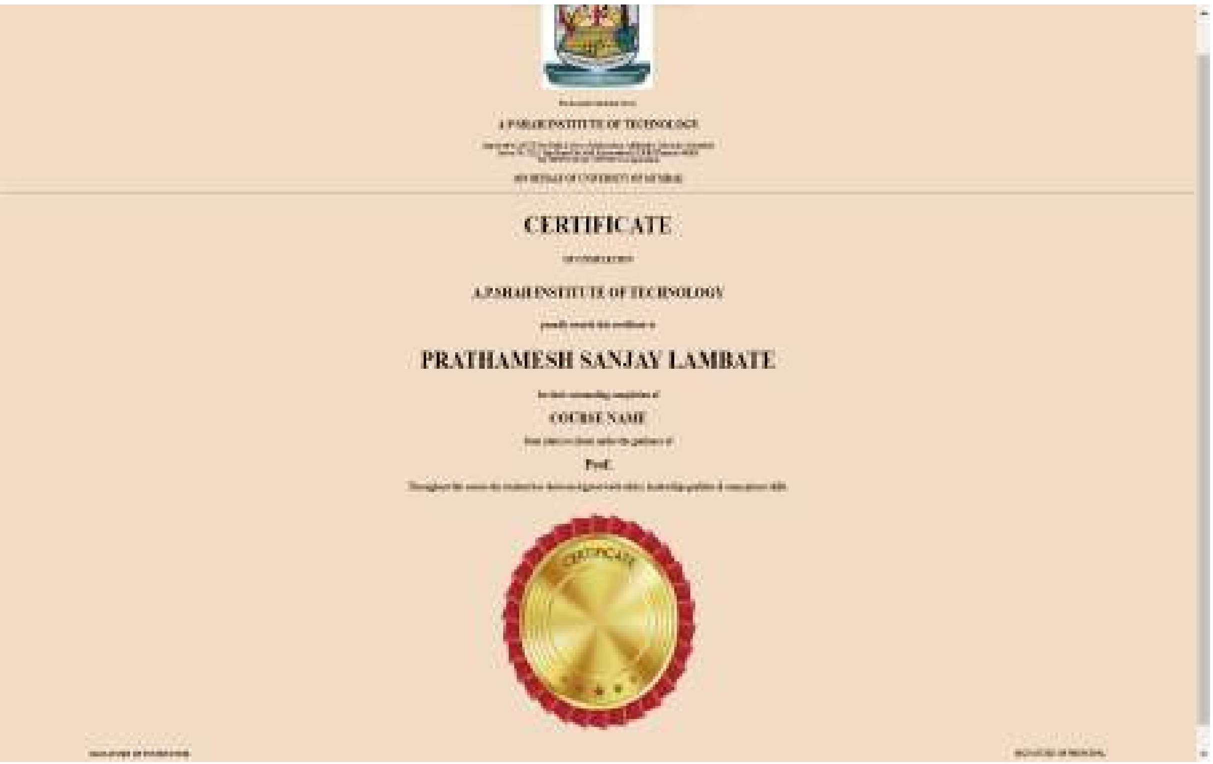
Click here to upload CSV file containing student data to generate certificates

APPRICIATION CERTIFICATE

Click here to upload CSV file containing student data to generate certificates

WINNER CERTIFICATE

Figure 6.9: Generate Certificates Page



[illegible]

A.P.SHAH INSTITUTE OF TECHNOLOGY

[illegible]

[illegible] UNIVERSITY OF MUMBAI

CERTIFICATE

[illegible]

A.P.SHAH INSTITUTE OF TECHNOLOGY

proudly awards this certificate to

PRATHAMESH SANJAY LAMBATE

for their outstanding completion of

COURSE NAME

[illegible]

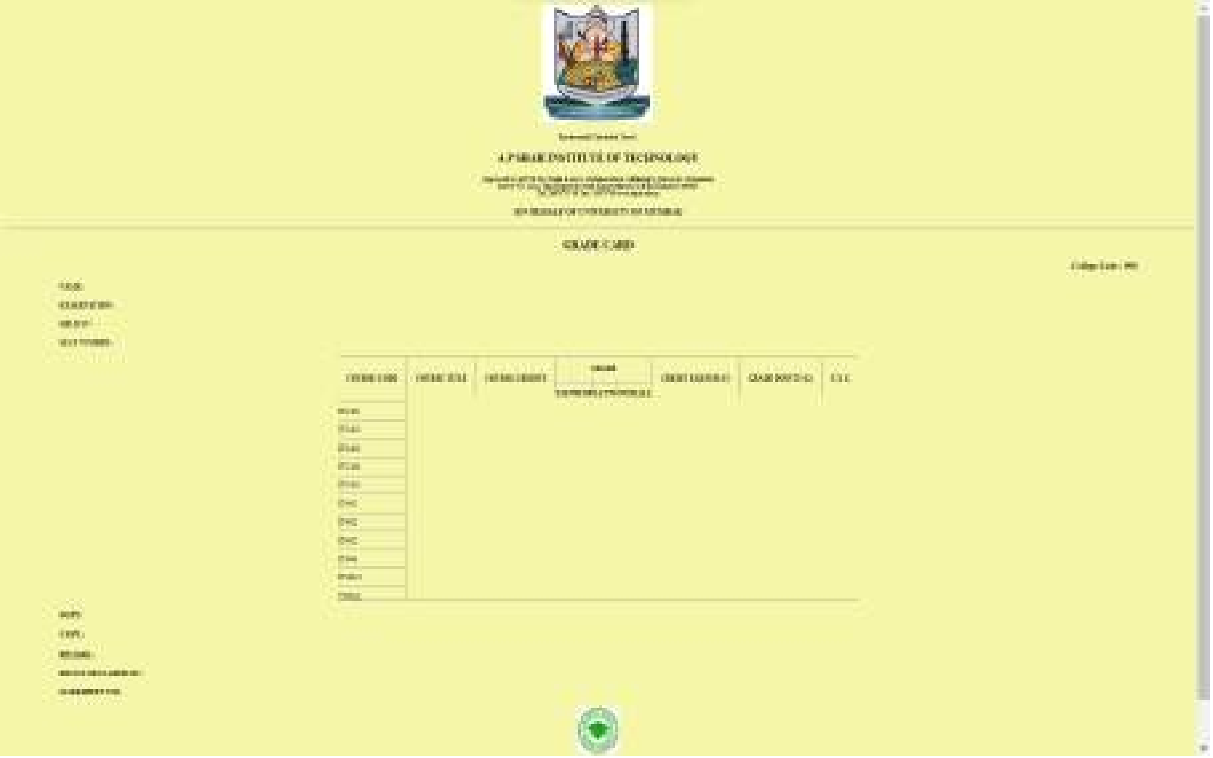
Prof.

[illegible]

SIGNATURE OF [illegible]

SIGNATURE OF PRINCIPAL

Figure 6.10: Certificate Template



[illegible]

A P SHAH INSTITUTE OF TECHNOLOGY

[illegible]

(ON BEHALF OF UNIVERSITY OF MUMBAI)

GRADE CARD

College Code : [illegible]

NAME :

EXAMINATION :

ROLL NO :

SEAT NUMBER :

COURSE CODE	COURSE TITLE	COURSE CREDIT	GRADE	CREDIT EARNED (C)	GRADE POINTS (G)	C x G
			[illegible]			
[illegible]						
[illegible]						
[illegible]						
[illegible]						
[illegible]						
[illegible]						
[illegible]						
[illegible]						
[illegible]						
[illegible]						
TOTAL						

SGPI :

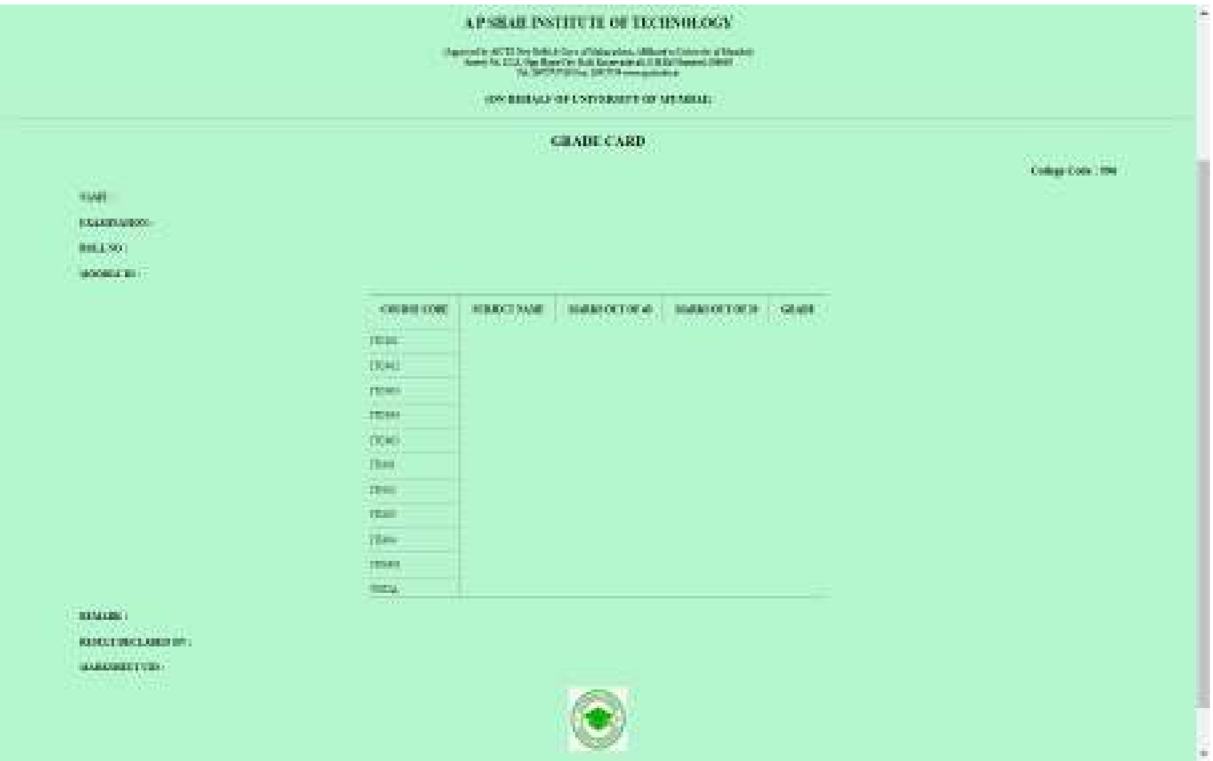
CGPI :

REMARK :

RESULT DECLARED ON :

MARKSHEET UID :

Figure 6.11: Marksheet Template 1



A P SHAH INSTITUTE OF TECHNOLOGY

[illegible]

(ON BEHALF OF UNIVERSITY OF MUMBAI)

GRADE CARD

College Code : 596

NAME :

EXAMINATION :

ROLL NO :

MOODLE ID :

COURSE CODE	SUBJECT NAME	MARKS OUT OF 40	MARKS OUT OF 20	GRADE
[illegible]				
[illegible]				
[illegible]				
[illegible]				
[illegible]				
[illegible]				
[illegible]				
[illegible]				
[illegible]				
[illegible]				
TOTAL				

REMARK :

RESULT DECLARED ON :

MARKSHEET UID :

Figure 6.12: Marksheet Template 2

Chapter 7

Conclusion

In conclusion, the development of a Comprehensive Certificate Validation and Verification System (CVVS) for educational institutes utilizing blockchain technology, specifically leveraging Ethereum, presents a transformative solution to the challenges plaguing traditional certificate management systems. By harnessing the decentralized and immutable nature of blockchain, coupled with Ethereum's smart contract capabilities, the proposed system offers a secure, transparent, and efficient means of issuing, storing, and validating educational certificates.

Through the integration of Ethereum smart contracts, the CVVS automates and streamlines the certificate management process, reducing administrative overhead, enhancing security, and improving trust among stakeholders. The system provides a reliable and tamper-proof record of certificate authenticity, mitigating the risk of fraud and counterfeit credentials. Moreover, by promoting transparency and decentralization, the CVVS fosters a culture of trust and accountability within the educational ecosystem.

In essence, the Comprehensive Certificate Validation and Verification System represents a significant step towards modernizing and enhancing the integrity of certificate issuance and verification processes. By embracing blockchain technology and Ethereum smart contracts, educational institutes can establish a secure and reliable framework for credentialing, paving the way for a more transparent, trustworthy, and efficient educational ecosystem.

Overall, our Comprehensive Certificate Validation and Verification System is a crucial component in creating a transparent, efficient, and student-focused educational environment. Embracing innovation and emerging technologies opens up possibilities for academic credentials to serve as gateways to personalized learning and professional success. This system will help to ensure the safety and legitimacy of the learning process, allowing students to pursue their educational goals with confidence. Furthermore, it will provide educational institutions with a powerful tool to track student progress and provide valuable insights into the learning process.

Chapter 8

Future Scope

The CVVS (Certificate Validation and Verification System) can benefit from various enhancements, including integration with other blockchains to enable greater flexibility and scalability, the integration of privacy-preserving techniques to improve the privacy of certificate holders, integration with identity management systems to manage and verify the identities of certificate holders, implementing mechanisms for certificate revocation to enhance the security of the system, leveraging machine learning algorithms for fraud detection, collaborating with international educational organizations and standards bodies to establish global standards, expanding the scope of the system to include academic records and transcripts, exploring the issuance and validation of blockchain-based diplomas and micro-credentials, community engagement and education, and investing in research and development initiatives to explore emerging technologies and best practices in blockchain-based certificate validation and verification.

Bibliography

[1] A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, ”A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification,” in IEEE Access, vol. 11, pp. 64679-64696, 2023, doi: 10.1109/ACCESS.2023.3289598.

[2] Devdoot Maji, Ravi Singh Lamkoti , Hitesh Shetty , Bharati Gondhalekar, 2021, Certificate Verification using Blockchain and Generation of Transcript, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 10, Is-sue 03 (March 2021).

[3] Doğan and H. Karacan, ”A Blockchain-Based E-Commerce Reputation System Built With Verifiable Credentials,” in IEEE Access, vol. 11, pp. 47080-47097, 2023, doi: 10.1109/ACCESS.2023.3274707.

[4] Rama Reddy, T., Prasad Reddy, P.V.G.D., Srinivas, R. et al. Proposing a reliable method of securing and verifying the credentials of graduates through blockchain. EURASIP J. on Info. Security 2021, 7 (2021). https://doi.org/10.1186/s13635-021-00122-5.

[5] H. Gaikwad, N. D'Souza, R. Gupta and A. K. Tripathy, ”A Blockchain-Based Verification System for Academic Certificates,” 2021 International Conference on System, Computa-tion, Automation and Networking (ICSCAN), Puducherry, India, 2021, pp. 1-6, doi: 10.1109/ICSCAN53069.2021.9526377.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, ”An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” 2017 IEEE International Congress on Big Data (Big Data Congress), Honolulu, HI, USA, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.

[7] J. -C. Cheng, N. -Y. Lee, C. Chi and Y. -H. Chen, ”Blockchain and smart contract for digital certificate,” 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, Japan, 2018, pp. 1046-1051, doi: 10.1109/ICASI.2018.8394455.

[8] E. Nyaletey, R. M. Parizi, Q. Zhang and K. -K. R. Choo, ”BlockIPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability,” 2019 IEEE Interna-tional Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 18-25, doi: 10.1109/Blockchain.2019.00012.

[9] G. Malik, K. Parasrampuria, S. P. Reddy and S. Shah, ”Blockchain Based Identity Verifica-tion Model,” 2019 International Conference on Vision Towards Emerging Trends in Com-munication and Networking (ViTECoN), Vellore, India, 2019, pp. 1-6, doi: 10.1109/Vi-TECoN.2019.8899569.

Appendices

Appendix-I: Docker Download and Installation

Step 1: Update Your System
Before you begin, it's a good practice to update your system's package repository and upgrade your installed packages to their latest versions:

```
sudo apt update
sudo apt upgrade
```

Step 2: Uninstall Old Versions (if applicable)
If you have older versions of Docker installed, you may need to remove them. Use the following commands to uninstall previous versions:

```
sudo apt remove docker docker-engine docker.io containerd runc
```

Step 3: Install Dependencies
Install some necessary packages that allow apt to use packages over HTTPS:

```
sudo apt install apt-transport-https ca-certificates curl software-properties-common
```

Step 4: Add Docker Repository
Add Docker's official GPG key to your system:

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg — sudo gpg –dearmor
-o /usr/share/keyrings/docker-archive-keyring.gpg
```

Then, add the Docker repository:

Step 5: Install Docker
Update your package index and install Docker:

```
sudo apt update
sudo apt install docker-ce docker-ce-cli containerd.io
```

Step 6: Start and Enable Docker
Start the Docker service and enable it to start at boot:

```
sudo systemctl start docker
sudo systemctl enable docker
```

Step 7: Verify Docker Installation
You can verify that Docker is installed and running by running the following command:

```
sudo docker –version
```

Step 8: Run a Test Container
To verify that Docker can pull and run containers, you can run a simple test container:
sudo docker run hello-world

If everything is set up correctly, you should see a message indicating that your installation appears to be working.

Appendix-II: Tools and Development Frameworks

1. Truffle
Truffle is a development environment, testing framework, and asset pipeline for Ethereum smart contracts.

Step 1: Install Node.js and npm:
Truffle requires Node.js and npm (Node Package Manager) to be installed on your system. You can download and install them from the official website: Node.js Downloads.

Step 2: Install Truffle globally:
Open a terminal or command prompt and run the following npm command to install Truffle globally:
npm install -g truffle

Step 3: Verify Installation:
After installation, you can verify that Truffle is installed correctly by running:
truffle version
This command should display the installed Truffle version.

2. Remix IDE
Remix IDE is an online development environment for writing and deploying smart contracts on the Ethereum blockchain.

Installation Steps:
Remix IDE is a web-based tool and does not require installation. Simply visit the Remix IDE website: Remix, and you can start using it directly from your web browser.

3. Web3.js
Web3.js is a JavaScript library for interacting with the Ethereum blockchain.

Step 1: Install Web3.js:
Open a terminal or command prompt and run the following npm command to install Web3.js:
npm install web3

Step 2: Incorporate Web3.js into your project:
Once installed, you can incorporate Web3.js into your JavaScript project using require or

import statements.

4. Metamask
Metamask is a browser extension that allows users to interact with Ethereum-enabled websites and decentralized applications (DApps).

Step 1: Install Metamask Extension:
Visit the Chrome Web Store (for Google Chrome) or Firefox Add-ons (for Mozilla Firefox).
Search for "Metamask" and click on "Add to Chrome" (or "Add to Firefox") to install the extension.
Follow the on-screen instructions to set up your Metamask wallet.

Step 2: Configure Metamask:
Once installed, click on the Metamask extension icon in your browser.
Follow the prompts to create a new wallet or import an existing one.
Set up a password and back up your seed phrase securely.

5. Ganache
Ganache is a personal Ethereum blockchain for development purposes.

Step 1: Download Ganache:
Visit the official website: Ganache.
Download the appropriate version of Ganache for your operating system (Windows, macOS, or Linux).

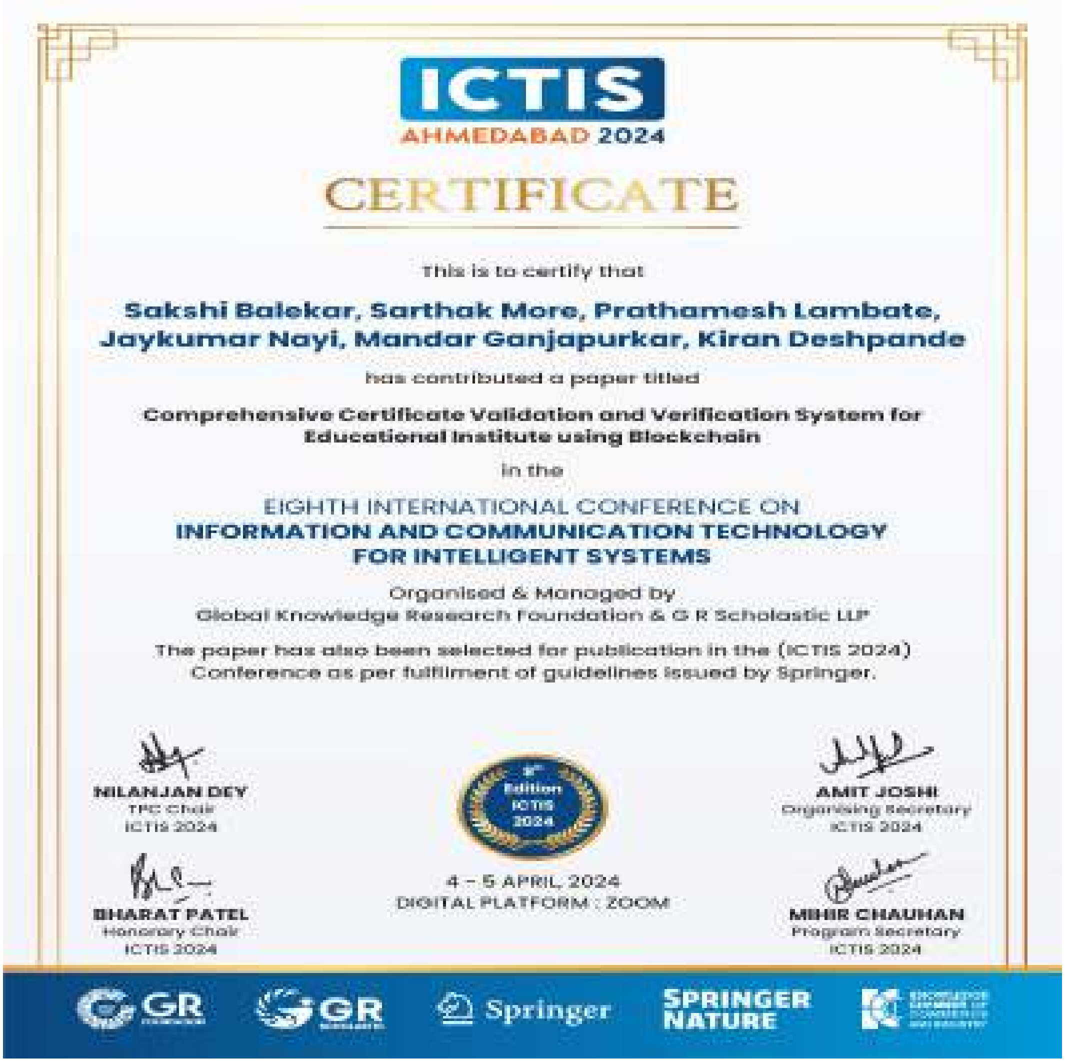
Step 2: Install Ganache:
For Windows: Double-click the downloaded .exe file and follow the installation instructions.
For macOS: Double-click the downloaded .dmg file and drag the Ganache application to your Applications folder.
For Linux: Extract the downloaded archive and run the ganache-¡version¿.AppImage file.

Step 3: Run Ganache:
Once installed, open Ganache from your applications menu.
Ganache will start a personal Ethereum blockchain locally on your machine, and you can use it for development purposes.

That's it! You've now installed Truffle, Remix IDE, Web3.js, Metamask, and Ganache. You're ready to start developing on the Ethereum blockchain.

Publication

Paper entitled **"Comprehensive Certificate Validation & Verification System for Educational Institute Using Blockchain"** is accepted at **"ICTIS 2024 - Ahmedabad and publication in Springer LNNS series"** by **"Sakshi Balekar, Sarthak More, Prathamesh Lambate, Jaykumar Nayi, Mr. Mandar Ganjapurkar and Dr. Kiran Deshpande."**.



ICTIS
AHMEDABAD 2024

CERTIFICATE

This is to certify that

Sakshi Balekar, Sarthak More, Prathamesh Lambate, Jaykumar Nayi, Mandar Ganjapurkar, Kiran Deshpande

has contributed a paper titled

Comprehensive Certificate Validation and Verification System for Educational Institute using Blockchain

in the

EIGHTH INTERNATIONAL CONFERENCE ON
INFORMATION AND COMMUNICATION TECHNOLOGY FOR INTELLIGENT SYSTEMS

Organised & Managed by
Global Knowledge Research Foundation & G R Scholastic LLP

The paper has also been selected for publication in the (ICTIS 2024) Conference as per fulfilment of guidelines issued by Springer.

NILANJAN DEY
TPC Chair
ICTIS 2024

8th Edition
ICTIS
2024

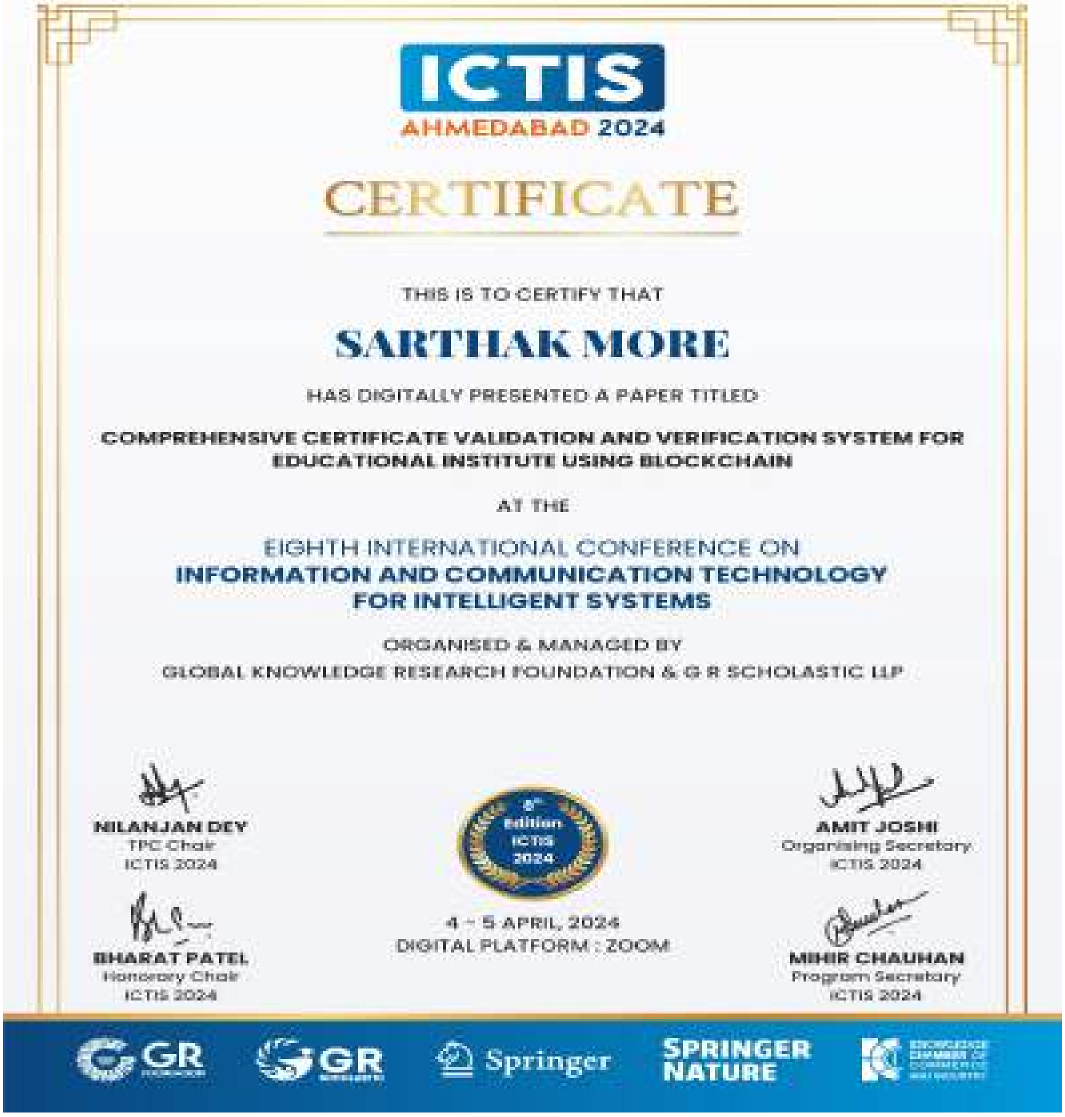
AMIT JOSHI
Organising Secretary
ICTIS 2024

BHARAT PATEL
Honorary Chair
ICTIS 2024

4 – 5 APRIL, 2024
DIGITAL PLATFORM : ZOOM

MIHIR CHAUHAN
Program Secretary
ICTIS 2024

Figure 8.1: Paper Publication



ICTIS

AHMEDABAD 2024

CERTIFICATE

THIS IS TO CERTIFY THAT

SARTHAK MORE

HAS DIGITALLY PRESENTED A PAPER TITLED

COMPREHENSIVE CERTIFICATE VALIDATION AND VERIFICATION SYSTEM FOR EDUCATIONAL INSTITUTE USING BLOCKCHAIN

AT THE

EIGHTH INTERNATIONAL CONFERENCE ON
INFORMATION AND COMMUNICATION TECHNOLOGY
FOR INTELLIGENT SYSTEMS

ORGANISED & MANAGED BY
GLOBAL KNOWLEDGE RESEARCH FOUNDATION & G R SCHOLASTIC LLP

NILANJAN DEY
TPC Chair
ICTIS 2024

8th Edition ICTIS 2024

AMIT JOSHI
Organising Secretary
ICTIS 2024

BHARAT PATEL
Honorary Chair
ICTIS 2024

4 - 5 APRIL, 2024
DIGITAL PLATFORM : ZOOM

MIHIR CHAUHAN
Program Secretary
ICTIS 2024

GR

GR

Springer

SPRINGER NATURE

Figure 8.2: Paper Presentation

Copyright for the software work titled **"EduMaster: Comprehensive Certificate Validation and Verification for Educational Institute using Blockchain"** is filed under **"Diary Number 7893/2024-CO/SW"** by **"Sakshi Balekar, Sarthak More, Prathamesh Lambate, Jaykumar Nayi, Mr. Mandar Ganjapurkar."**