SuperCert - An Anti-fraud Identity Intelligence Blockchain Solution for Educational certificates

(AY23BECSP80107)

A **Major Project Report** Submitted in partial fulfilment of the requirements of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER ENGINEERING

BY

Akanksha Gairola (Roll No. 41)

Shriya Salian (Roll No. 61)

Shankar Malve (Roll No. 48)

Amira Shaikh (Roll No. 29)

Supervisor
Mr. Pravin Jangid (Assistant Professor)
(Dept. of Computer Engineering)

DEPARTMENT OF COMPUTER ENGINEERING

Accredited by NBA for 3 years w.e.f. 1st July 2022

SHREE L. R. TIWARI COLLEGE OF ENGINEERING

SHREE L.R. TIWARI EDUCATIONAL CAMPUS, MIRA ROAD (East),
THANE -401 107, MAHARASHTRA.

University of Mumbai

(AY 2023-24)

Declaration by the Candidate

I/We declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I/We have adequately cited and referenced the original sources. I/We also declare that I/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 my submission. I/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.

Date: The______April, 2024

Akanksha Gairola
Roll No.:41 Exam. Seat No.:

Shriya Salian
Roll No.:61 Exam. Seat No.:

Shankar Malve
Roll No.:48 Exam. Seat No.:

Amira Shaikh
Roll No.:29 Exam. Seat No.:

Shree Rahul Education Society's (Regd.)

SHREE L. R. TIWARI COLLEGE OF ENGINEERING

Kanakia Park, Near Commissioner's Bungalow, Mira Road (East), Thane 401107, Maharashtra
(Approved by AICTE, Govt. of Maharashtra & Affiliated to University of Mumbai)
NAAC Accredited | ISO 9001:2015 Certified
Tel. No.: 022-28120144 / 022-28120145 | Email: slrtce@rahuleducation.com | Website: www.slrtce.in

DEPARTMENT OF COMPUTER ENGINEERING

Accredited by NBA for 3 years w.e.f. 1st July 2022

CSP801 Major Project – 2

Eighth Semester, 2023-2024 (Even Semester)

CERTIFICATE

This is to certify that the **Major Project** entitled **"SuperCert - An Anti-fraud Identity Intelligence Blockchain Solution for Educational certificates"** is a bonafide work of

Akanksha Gairola (Roll No. 41)

Shriya Salian (Roll No. 61)

Shankar Malve (Roll No. 48)

Amira Shaikh (Roll No. 29)

submitted to the University of Mumbai in partial fulfilment of the requirement of course name "**Major Project – 2**" having course code **CSP801** for the award of the degree of **"Bachelor of Engineering"** in **"Computer Engineering"**.

Signature of Supervisor/Guide	**Signature of Project Coordinator**
Name: Mr. Pravin Jangid	**Name: Dr. Vinayak D. Shinde**
Date:________________	**Date: ________________**
Signature of the H.O.D.	**Signature of the Principal**
Name: Mrs. Neelam Phadnis	**Name: Dr. Deven Shah**
Date:______________	**Date: ________________**

Shree Rahul Education Society's (Regd.)

SHREE L. R. TIWARI COLLEGE OF ENGINEERING

Kanakia Park, Near Commissioner's Bungalow, Mira Road (East), Thane 401107, Maharashtra

(Approved by AICTE, Govt. of Maharashtra & Affiliated to University of Mumbai)

NAAC Accredited | ISO 9001:2015 Certified

Tel. No.: 022-28120144 / 022-28120145 | Email: slrtce@rahuleducation.com | Website: www.slrtce.in

DEPARTMENT OF COMPUTER ENGINEERING

Accredited by NBA for 3 years w.e.f. 1st July 2022

CSP801 Major Project – 2

Eighth Semester, 2023-2024 (Even Semester)

Major Project Report Approval

This Mini-project report entitled "**SuperCert - An Anti-fraud Identity Intelligence Blockchain Solution for Educational certificates**" by

Akanksha Gairola (Roll No. 41)

Shriya Salian (Roll No. 61)

Shankar Malve (Roll No. 48)

Amira Shaikh (Roll No. 29)

is belonging to the course name "**Major Project – 2**" having course code **CSP801** submitted as a Term work and approved for the degree of Batchelor of Engineering in Computer Engineering.

Examiners

1. Name:_________________________(Internal)

   Signature: ______________________

2. Name:________________________(External)

   Signature: _____________________

Date:

Place:

Acknowledgement

I take this opportunity to express my profound gratitude and deep regards to my guide Mr. Pravin Jangid for her exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The help and guidance given by her from time to time shall carry me a long way in the journey of life on which I am about to embark. My special gratitude goes to the senior students and my teammates for helping me through this project. I would also like to extend my thanks to the technicians of the laboratory. Finally, I wish to thank my parents for their support and encouragement throughout my study.

Akanksha Gairola
Roll No.: 41 Exam. Seat No.:
Shriya Salian
Roll No.: 61 Exam. Seat No.:
Shankar Malve
Roll No.: 48 Exam. Seat No.:
Amira Shaikh
Roll No.: 29 Exam. Seat No.:

Abstract

In recent years, the proliferation of fraudulent educational certificates has posed significant challenges to academic institutions, employers, and individuals alike. Such certificates not only undermine the credibility of educational achievements but also jeopardize the integrity of various industries. To combat this issue, this research introduces SuperCert, an innovative anti-fraud identity intelligence blockchain solution tailored for educational certificates. SuperCert leverages blockchain technology to establish a decentralized, immutable ledger that securely stores educational credentials. SuperCert's decentralized structure implies that no central authority controls the system. Instead, educational credentials are distributed throughout a network of nodes, making it exceedingly impossible for a single party to falsify or corrupt the information. Once educational credentials are recorded on the SuperCert blockchain, they cannot be altered or deleted. This immutability ensures that certificates remain trustworthy and verifiable over time. The system incorporates smart contract functionality to automate verification processes, thereby reducing administrative overhead and enhancing efficiency.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

API	Application programming interfaces
CID	Content Identifier.
IPFS	InterPlanetary File System
UML	Unified Modeling Language

1 Introduction

1.1 Introduction

Certificates' are a means of verifying the credentials of individuals across domains and geographies. A paper-based certification is fallible to manipulation and susceptible to fraud. According to a report by First Advantage, a background screening company, there are more than 7,500 organizations that provide fake employment and educational certificates.

The proliferation of fraudulent educational certificates has become a widespread concern, casting a shadow on the integrity of academic institutions and the professionals they graduate. There are usually two problems at play: Degrees from fake universities and fake degrees from real universities. For higher Education the other organization verifies it by approaching universities, and university approaches to colleges which can be very time consuming.

Proposed blockchain solution can be used as a mechanism to verify the degree obtained by the students. Supercert resolves the issues, including, utilizing a multi-signature scheme to ameliorate the authentication of certificates; exerting a safe revocation mechanism to improve the reliability of certificates revocation; establishing a secure federated identification to confirm the identity of the issuing institution.

1.2 Background and Motivation

The genesis of SuperCert emerged from a critical examination of the persisting challenges in the realm of educational certificate verification. The prevalence of counterfeit diplomas and fake certificates had reached alarming proportions, casting doubt on the credibility of academic achievements and the institutions that awarded them. The traditional method of paper-based certificates is susceptible to manipulation, forgery, and misrepresentation. This not only undermines the credibility of educational institutions but also poses risks to employers, students, and other stakeholders who rely on accurate and verified educational credentials. The motivation behind SuperCert, an anti-fraud identity intelligence blockchain solution for educational certificates, stems from the need+ to address these challenges and establish a secure, tamper-proof, and transparent system for verifying educational credentials. The proliferation of fraudulent certificates undermined the hard work and dedication of genuine students and the reputation of reputable institutions. This solution aims to leverage the unique properties of blockchain technology to enhance the trustworthiness and authenticity of educational certificates.

1.3 Problem statement

The development of a blockchain application that enables educational institutions to preserve immutable transcript records for their students necessitates the creation of an accessible user interface for administrators and students alike. After courses are finished or academic milestones are reached, administrators enter relevant data into the application, which generates digital transcripts that are time stamped and cryptographically signed. Together with their cryptographic signatures, these transcripts are securely stored on a blockchain network, ensuring transparency and immutability. Afterwards, by obtaining access to the blockchain and confirming the veracity of transcripts, corporations can view comprehensive academic records with cryptographic proof of integrity. Data security and privacy are given top priority by the program through the use of robust encryption and access controls. Scalability and interoperability are important considerations since they can handle various data volumes and interact with existing academic systems with ease. Ongoing technical support and maintenance ensure smooth operation, maximizing adoption and usefulness. All things considered, this blockchain application assists students and companies who verify educational qualifications by enhancing the security, transparency, and dependability of academic information. The current methods are functional, but since the process often takes several weeks, efficiency and security need to be increased. This is costly and environmentally damaging, in addition to being inconvenient and time-consuming. The solution to this problem is to recognize fake certificates, store certificates, and streamline the internal verification process of an organization's certificates without using a third party.

1.4 Project Objectives

1. Develop a digital ledger to store the degree information about the students graduated from the college.
2. To promote efficiency for other institutions and organizations to verify the student’s degree.
3. The objective is to create a solution that can be adopted globally, that will be an accurate and immutable record.
4. Its aim is to minimize verification delays that often occur with manual processes.
5. To create a unique hash or QR code for each and every document of students enrolled in the college as an immutable entity.
6. Store , manage and upload student information and documents in a way that meets the blockchain requirements (transparency, proof of consensus).
7. To restore trust and credibility in the education verification process, ensuring that qualifications are accurately represented and recognized.
8. To promote lifelong learning and application of concepts to develop real world solutions.
9. To develop a blockchain using IPFS protocol to store documents.

1.5 Project Importance

1. The college admin will have to login through their wallet id.
2. The application is responsible for the main logic which includes the transcript signing and issuing. The application will be designed to merge the hash of the transcript in a Merkle tree and send the Merkle root to Blockchain, amidst signing by the majority of community members.
3. The application will be used by the organization to store student performance information, which can be uniquely identified by hash and QR code (degree, grade card), and by external institutions to verify the same.

1.6 Scope of Project Work

The scope of this project includes the development of a web-based interface for the Anti-fraud Identity Intelligence Blockchain Solution for educational certificates.

1. The proposed application will be a private blockchain, only allowing verified members to add information blocks to the blockchain.
2. The system is intended to help us create the digital relationship that will reshape the world of education and transform the old order of human affairs for the better.
3. Documents will be identified based on their assigned hash and QR code, which will be sent to the student's email- address assigned by their college.
4. The system will be designed using React, with a backend powered by Node.js, IPFS protocol, and database.

1.7 Organization of the Report

The report is divided into six parts. Each part deals with the different aspects. Each part has various chapters explaining in detail.

Part 1: Introduction
Highlight the evolving nature of education and the increasing reliance on digital credentials.
Introduce SuperCert as an innovative solution designed to address the challenges associated with fraud in educational certificates.

Part 2: Motivation
Explanation of the driving factors behind the development of SuperCert.

Part 3: Problem Statement
Description of the prevalent issues related to fraud in educational certificates.

Part 4: Project Objective
Clear articulation of the goals and objectives that SuperCert aims to achieve.
Highlight the intended impact of SuperCert on enhancing the integrity and trustworthiness of educational credentials.

Part 5: Project Importance

Discuss the broader significance of SuperCert within the context of education.

Illustrate how SuperCert contributes to building a more secure and reliable credentialing system.

Part 6: Scope of Project Work

Define the boundaries and limitations of the SuperCert project. Provide a comprehensive understanding of the specific focus areas and deliverables of the SuperCert solution.

2 Literature Review

2.1 Survey of Existing System

In 2022, Pathak, Shivani, et al in their paper "Blockchain-based academic certificate verification system—a review" [6]. A proposed approach shows the Bird eye view to the process of academic certificate storage and verification process review, web3js used for blockchain hash verification and strong digital signature used to hash the document.

In 2022, Krishna Bihari Dubey and Mukta Goyal in their paper “Smart Certificate using Blockchain”[3].This study aims to use blockchain to create safe Smart Certificates. It offers a viable alternative for issuing, confirming, and exchanging certificates without fear of their integrity being compromised.

In 2021, Bele, Roshani S., and Jayant P. Mehare in their paper "A review on digital degree certificate using blockchain technology" [7]. Proposed a systematic representation of the academic certificate verification using ER diagrams, use cases etc.

In 2020, Ashis Kumar Samanta, Bidyut Biman Sarkar & Nabendu Chaki in their paper “A Blockchain-Based Smart Contract Towards Developing Secured University Examination System”[10]. Proposed a comprehensive survey on smart contracts is carried out. It also present a case study on a University examination system having a heterogeneous data structure. The deployment brings a comprehensive understanding of the smart contract framework and has been used to find and analyze the gaps in the state of the art in terms of smart contracts.

In 2021, Nero Chaniago a Parman Sukarno b , Aulia Arif Wardana c in their paper “ “Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain”[24]. The system uses Ethereum blockchain to verify electronic documents like diplomas and transcripts, preventing fraud and simplifying verification. Electronic files replace print versions, reducing paper use. Each file's integrity is preserved, ensuring any alterations are detected. Blockchain transparency reduces document falsification by handling publication and verification, ensuring accurate information.

In 2020, OMAR S. SALEH, OSMAN GHAZALI, MUHAMMAD EHSAN RANA in their paper “Blockchain based framework for Education certificate verification” [25]. This research discussed the security themes required for educational certificates verification in the blockchain. In addition to that, blockchain-based framework for educational certificate verification focusing on specific themes is proposed based on Hyperledger Fabric Framework.

In 2023, K. V Raghavender(B) , S. Alankruthi, A. Akhila, T. Preethi, and M. Ashritha in their paper “Decentralised Smart Contract Certificate System Using Ethereum Blockchain Technology” [23]. The proposed solution establishes a federated blockchain system for businesses, academic institutions, and students. It streamlines certificate verification, prevents data tampering, and reduces manual effort. Using SHA2–256 hashing, it ensures data integrity. The InterPlanetary File System stores documents, while the blockchain stores certificate hashes, ensuring transparency. Future directions include expanding authentication systems and eliminating fraudulent certificates.

2.2 Problems with Present System

Manual Verification Process:

Time-Consuming: Manual verification of educational certificates can be a time-consuming process, especially for organizations receiving a high volume of certificates.

Prone to Human Error: Relying on manual processes increases the risk of human error in verifying and recording certificate information.

Certificate Fraud and Forgery:

Ease of Forgery: Traditional certificates are susceptible to forgery or alteration, leading to instances of fraudulent claims and misrepresentations.

Limited Transparency and Traceability:

Lack of Transparency: Stakeholders often have limited visibility into the certificate issuance and verification process, leading to trust issues.

Privacy and Data Security Concerns:
Risk of Data Breaches: Storing sensitive educational data in traditional databases may expose it to potential security breaches

2.3 Limitation existing system or research gap

Traditional certificates are susceptible to forgery or alteration, leading to instances of fraudulent claims and misrepresentations.
Difficulty in Tracking Certificate Issuance and Verification History:
The current system may lack a transparent and immutable ledger to track the history of certificate issuance and verification.

Data Privacy and Security Concerns:
Storing sensitive educational data in traditional databases may expose it to potential security breaches and privacy risks.

2.4 Major project Contribution

SuperCert employs blockchain technology and cryptographic techniques to create a tamper-proof ledger, making it extremely difficult for fraudsters to alter or forge educational certificates. The blockchain ledger provides a transparent and immutable record of certificate issuance and verification, enhancing trust between certificate issuers, verifiers, and recipients. SuperCert is designed for seamless integration with existing educational systems and platforms, minimizing disruption to current workflows.
SuperCert's blockchain ledger maintains a permanent record of all certificate issuance and verification events, creating a comprehensive and auditable history. SuperCert encourages continuous education and professional development by providing a secure platform for individuals to validate their achievements and credentials.

3 Proposed System

3.1 Introduction

The proposed system addresses the critical issues surrounding the storage and authentication of student degree information. It achieves this by integrating blockchain technology with the InterPlanetary File System (IPFS), creating a secure, immutable, and efficient platform for storing and verifying educational records on a global scale.

The system operates by allowing institutions and authorized users to securely upload student documents, such as transcripts, diplomas etc. Each document is assigned a unique cryptographic hash and a corresponding QR code, facilitating quick and reliable verification. Once a document is successfully uploaded, the system automatically sends a copy to the respective student via email or a secure messaging system, ensuring they have immediate access to their records. This process streamlines the distribution of educational credentials and increases transparency.

The use of blockchain technology is central to the system's effectiveness. By recording all transactions and document uploads on an immutable blockchain ledger, the system eliminates the risk of tampering or unauthorized alterations. This decentralized approach removes the need for a central authority, such as universities or colleges, to manage educational records. Instead, the blockchain serves as a public and unchangeable source of truth, reducing the reliance on centralized servers that can be prone to breaches or data loss.

Additionally, the InterPlanetary File System (IPFS) is used to store student documents. This decentralized protocol allows files to be distributed across a global network, ensuring redundancy and high performance. IPFS also provides Content Identifiers (CIDs), unique labels that point to specific content on the network. These CIDs can serve as proof of work for transcripts, providing a verifiable link between the document and its corresponding blockchain record.

SuperCert, an integral component of this system, offers educational institutions the ability to register on the platform and securely issue digital certificates upon program completion. The platform's real-time verification system allows instant validation of certificates by educational institutions, employers, or any authorized third-party verifier. This functionality enhances the credibility and trustworthiness of the educational credentials, allowing employers and other stakeholders to quickly confirm the authenticity of a given document.

SuperCert's approach to verification relies on smart contracts, which automate the validation process. Smart contracts contain pre-defined rules that ensure consistency and integrity in the verification process. This automation reduces delays and eliminates the need for manual checks, further enhancing efficiency and reliability.

The system's robust security measures safeguard user privacy and data. Encryption is employed to protect sensitive information, and access controls restrict document access to authorized users only. The platform also includes anti-fraud measures to combat fraudulent activities, such as fake degrees or transcripts, ensuring the system's integrity.

By leveraging blockchain technology, the system achieves global recognition for educational credentials. Students and alumni can easily share their documents with employers and other institutions, facilitating international mobility and promoting lifelong learning. Furthermore, the decentralized verification system provided by SuperCert ensures trustworthiness and transparency, positioning it as a comprehensive solution for combating fraud in educational certificates.

3.2 Requirement Analysis

Functional Requirements:

Sr.no	Function	User Story	Requirements	Priority
1	Admin Login	As an existing user, I want to be able to log into my account.	The system must allow admin to log into their account by entering their college email id and password.	Must have
2	Upload pdf files	As an existing user, I want to be able to upload pdf files.	The system must allow user to upload pdf files.	Must have
3	Generation of Hash Value	As an existing user, I want generation	The system must correctly process the information to load unique Hash Value.	Must have

		of unique Hash Value of respective document.		
4	Mail Hash Value to respective student.	The generated hash must be sent to respective student email id.	The system upon generating the unique Hash should be automatically mailed to respective student email.	Must have
5	Provide Strong Hash Value	As an existing user, I want my generated digital signature to be unique and strong.	The system must provide unique and strong digital signature.	Must have

Table 3-1 : Functional Requirements

Non-Functional Requirements:

CORRECTNESS: The system should generate a valid and appropriate hash and QR code for every student.

MAINTAINABILITY: The system should maintain all the records as well as the multiple digital signatures.

USABILITY: The system should satisfy the maximum number of users' needs.

3.3 Architecture

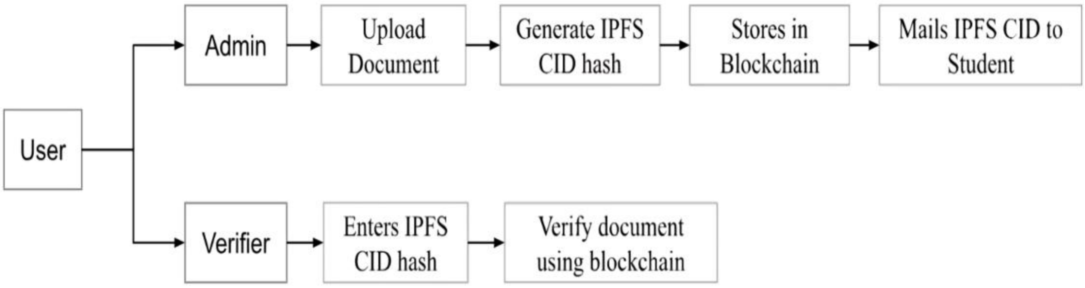


Figure 3-1 : System Architecture

The two modules of the system are Verifier and Admin. Transcripts of students are uploaded and stored on the blockchain by the administration. The IPFS CID will be mailed to the esteemed student via the system.

Higher education institutions or the organization itself may act as the Verifier, using the provided hash to validate the transcript. This removes the need for third parties and the verification time.

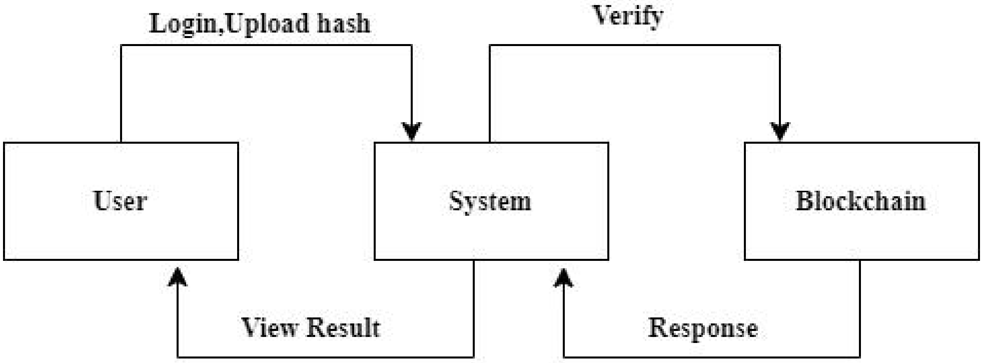


Figure 3-2 : Verifier Architecture

The verifier must input their name, email address, branch, student name, email address, and verification organization as their login, all of which will be stored in the database. Following entry of the cid hash, the system verifies the data from the blockchain and, if the credentials are correct, opens the PDF; if not, it returns the user to the system.

3.4 Framework

Project frameworks are organized plans that guarantee a project's effective completion and are used to plan, initiate, manage, and complete a project while adhering to all the required processes. It encompasses all the key components required for planning, managing, and governing projects.

It consists of five phases:

1. Initiation: The problem statement is defined in accordance with the real-world issue during the first part of the framework, and the project is created accordingly.
2. Planning: We plan and design the project architecture, sequence diagram and

other

3. necessary elements during this period to ensure the success of our project.
4. Execution: In this phase it includes coding of modules. Frontend and backend is
5. created. After successful creation of modules it is integrated and executed all at once.
6. Monitoring and controlling: The product is checked for all bugs and errors after it has been completed.
7. Closure: The final phase incorporates the results achieved when all project tasks are completed.

3.5 Algorithm

The hashing algorithm's core principle is the fact that transforms any length of data into a fixed length, which greatly simplifies the act of storing and looking for blocks while still ensuring security.

The proposed system's algorithm is as follows:

1. The certificate will be uploaded by the user.
2. Information such as the user's it will be extracted the name, and email id.
3. The extracted data will be hashed.
4. The hash will be looked for in the blockchain.
5. Certificate is valid if such a hash exists.

3.6 Details of Hardware & Software

Software used:

1. VS Code
2. Node.js
3. Remix IDE
4. React
5. Solidity
6. Bootstrap

Hardware used:

For Developers:

1. Hard Disk Space of minimum 20GB.
2. Windows XP, Windows 7 etc.
3. Minimum 4GB RAM for database server.
4. Windows Internal 5GB minimum for IDE's and Server functioning.

For Users:

1. Windows XP or any compatible versions.
2. 4GB Internal Space for working of application

3.7 Design details

To implement the proposed blockchain-based system for storing and verifying student degree information, we need to consider several key design aspects, including dataflow diagram, structural UML diagram and behavioral UML diagram.

3.7.1 Data Flow Diagram

A data-flow diagram is a way of representing a flow of data through a process or a system (usually an information system). The DFD also provides information about the outputs and inputs of each entity and the process itself. A data-flow diagram has no control flow — there are no decision rules and no loops. Specific operations based on the data can be represented by a flowchart.

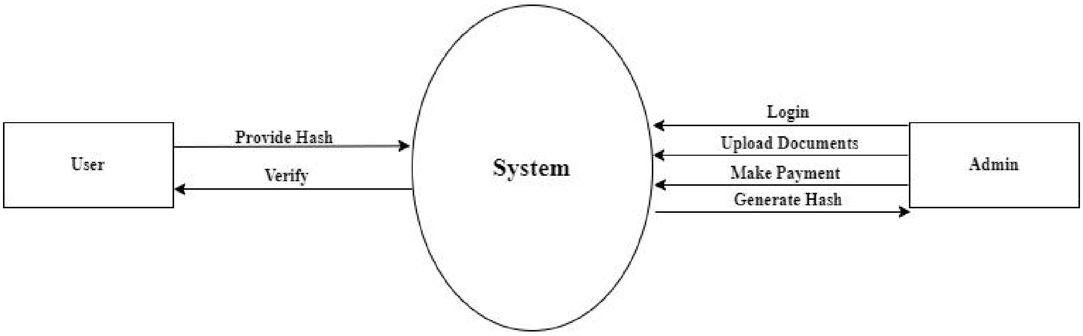


Figure 3-3 : DFD Level 0

User or Verifier:

In order for the system to verify the document, they must supply the CID hash.

Admin:

In order to access the admin dashboard, they must supply their login credentials. In order for the transcript document to be successfully uploaded and stored in the blockchain, they must also pay. Subsequently, the system will email the students' addresses and record them in a database.

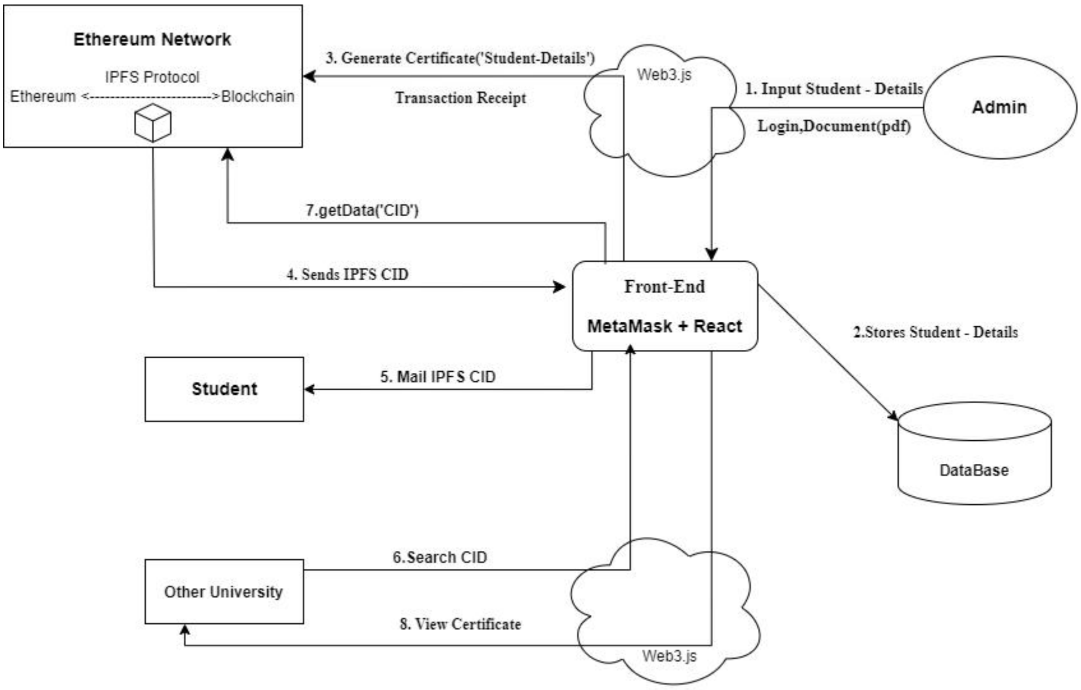


Figure 3-4 : DFD Level 1

The sequence begins with:

1. The administrator with the authority to upload transcripts. Will begin with logging into the system, entering all of the student's credentials, and uploading a document in PDF format that is no more than 10 MB.

2. After the administrator finished his payment successfully, these details were entered into the database.

3. The Ethereum network is used to generate and store the IPFS CID hash, or certificate transcript receipt.

4. The system receives the IPFS CID from Blockchain.

5. The corresponding student mail will receive these CID hashes.

When Higher Educational University tries to confirm the transcript of the student:

6. The university will look for the hash that a student submitted to them. The university needs to pay for verification as well.

7.The system will obtain the document after the payment has been finished.

8. University can now see the information.

3.7.2 Use Case

A Use Case Diagram is a vital tool in system design, it provides a visual representation of how users interact with a system. It serves as a blueprint for understanding the functional requirements of a system from a user's perspective, aiding in the communication between stakeholders and guiding the development process.

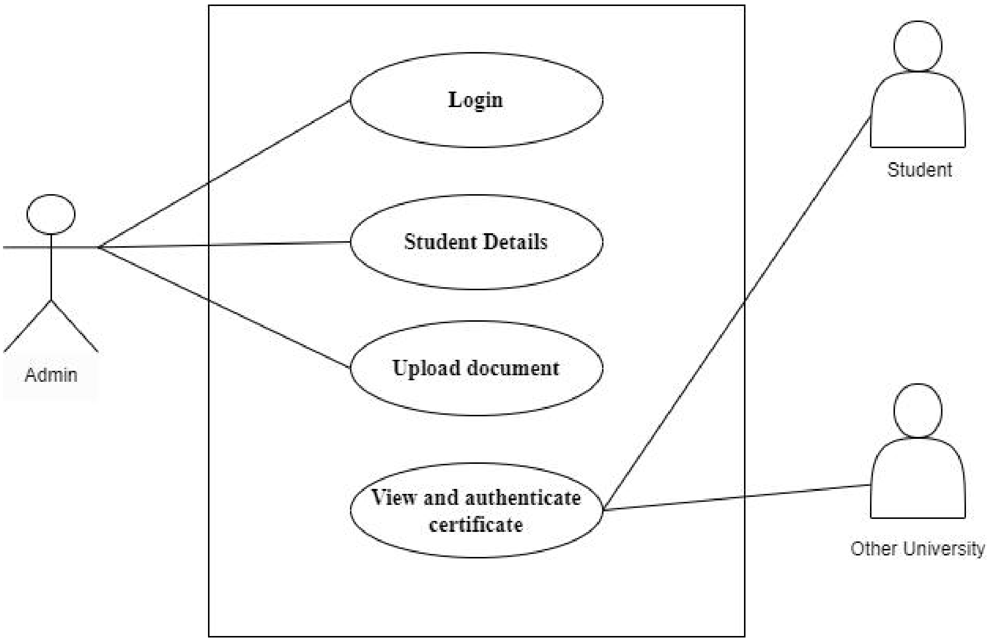


Figure 3-5 : Use Case

Functionality:

Students and higher education institutions are only authorized to access and authenticate the certificate.

For Admin: They are authorized to upload the student transcript document, enter student information, handle files, and maintain system logs.

3.7.3 Structural UML Diagram

Class diagrams are a type of UML (Unified Modeling Language) diagram used in software engineering to visually represent the structure and relationships of classes in a system. UML is a standardized modeling language that helps in designing and documenting software systems. They are an integral part of the software development process, helping in both the design and documentation phases.

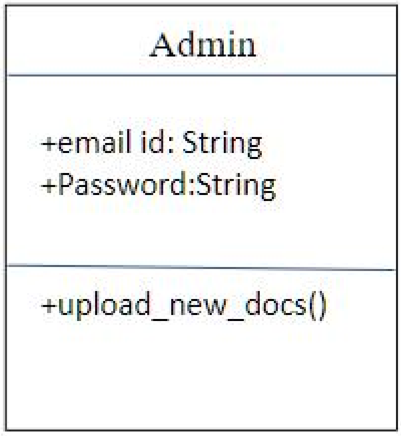
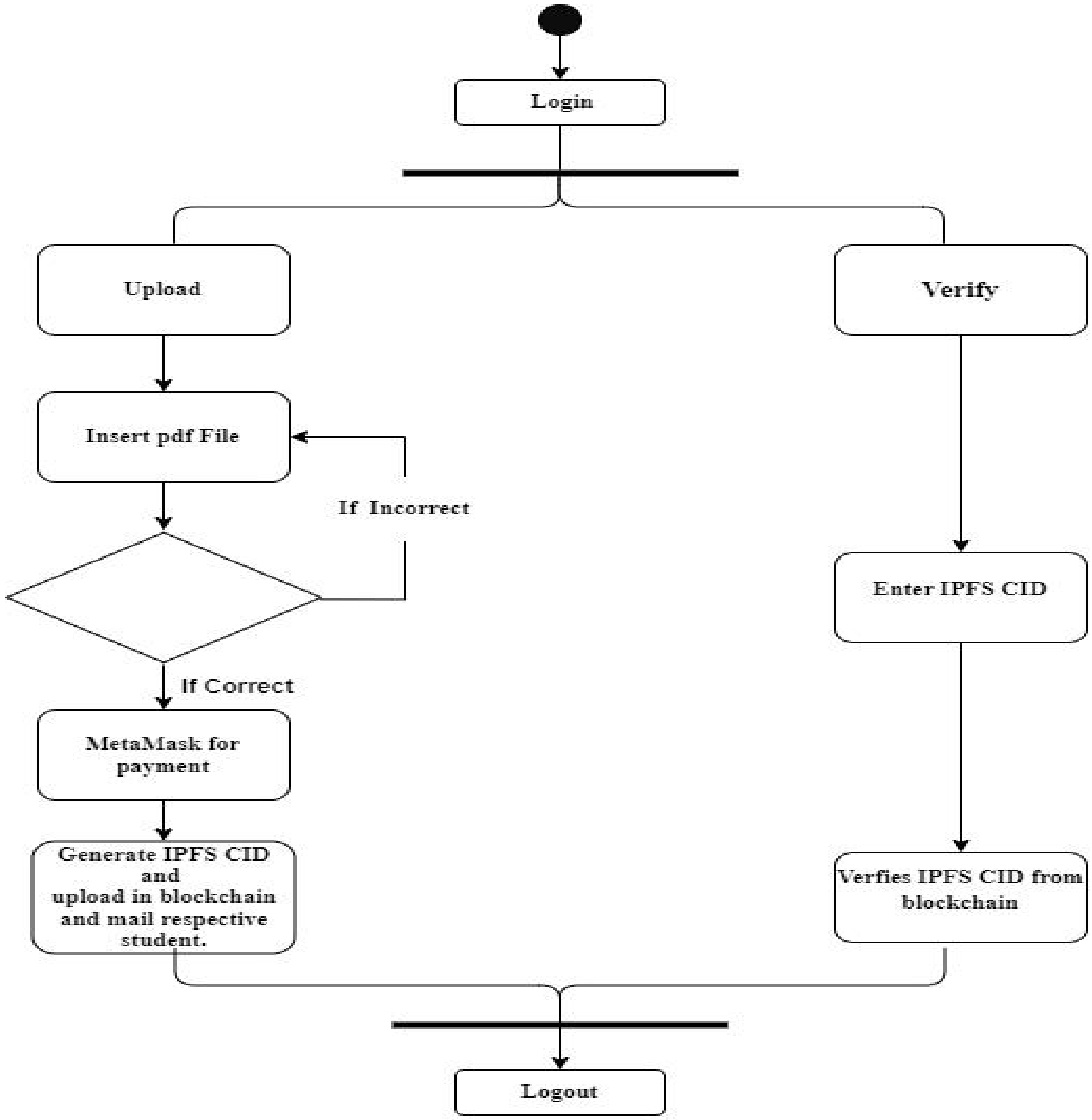


Figure** 3-6* ***: Class Diagram

The system has only class diagram for admin where they have to enter email and password as string. And have upload new document function for further process.

3.7.4 Behavioral UML diagram

An activity diagram visually presents a series of actions or flow of control in a system similar to a flowchart or a data flow diagram. Activity diagrams are often used in business process modeling. They can also describe the steps in a use case diagram. Activities modeled can be sequential and concurrent. In both cases an activity diagram will have a beginning (an initial state) and an end (a final state).



Login
Upload
Verify
Insert pdf File
If Incorrect
If Correct
Enter IPFS CID
MetaMask for payment
Generate IPFS CID and upload in blockchain and mail respective student.
Verfies IPFS CID from blockchain
Logout

Figure** 3-7 **: Activity Diagram

There are two primary modules here:

Upload: The initial action an administrator is authorized to take upon a successful login.The system is now initialized and ready to accept documents.

Insert: The document needs to be uploaded at this point. Any document submitted that is not in PDF format or that is more than 10 MB will result in an error and a return to the upload state.

Using Metamask to make payments: The administrator must pay once the material has been successfully uploaded. In the event of a cancellation or insufficient funds, the procedure will end and the upload status will be restored.

If the aforementioned procedures are carried out successfully, an IPFS CID is created, posted to the blockchain, and mailed to the appropriate student.

Validate: Students and other higher education institutions typically utilize this module to authenticate and validate the transcript. It asks to enter the student credential in this state.
It will request payment if the entered credential is found in the blockchain; else, it will return to the verify state.

Confirms IPFS CID from blockchain: This state is entered once a successful payment has been made. The document is provided with the verifier after verification.

In software engineering, a sequence diagram or system sequence diagram (SSD) shows process interactions arranged in a time sequence. The diagram depicts the processes and objects involved and the sequence of messages exchanged as needed to carry out the functionality. Sequence diagrams are typically associated with use case realizations in the 4+1 architectural view model of the system under development. Sequence diagrams are sometimes called event diagrams or event scenarios.

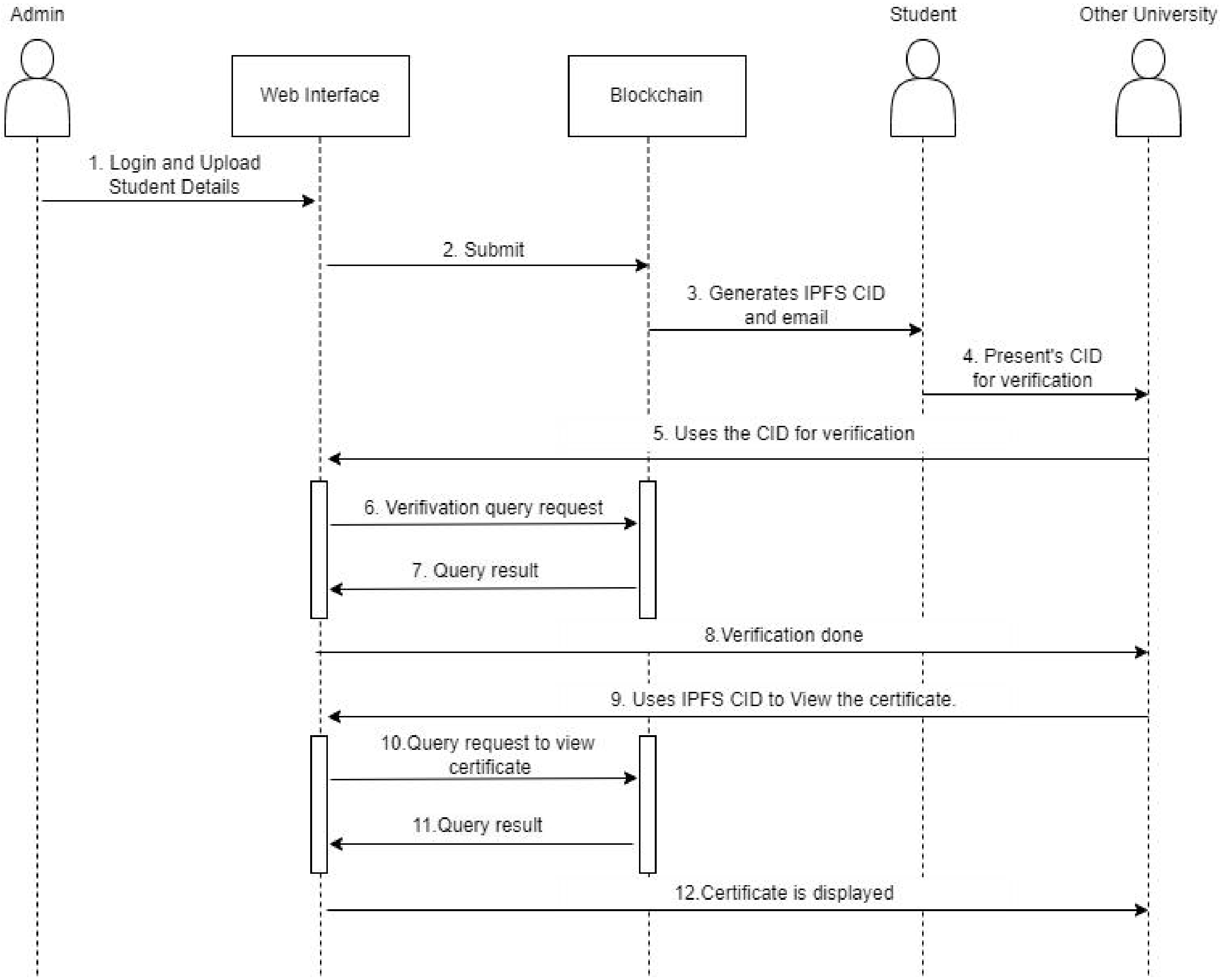

Admin
Student
Other University
Web Interface
Blockchain
1. Login and Upload Student Details
2. Submit
3. Generates IPFS CID and email
4. Present's CID for verification
5. Uses the CID for verification
6. Verifivation query request
7. Query result
8.Verification done
9. Uses IPFS CID to View the certificate.
10.Query request to view certificate
11.Query result
12.Certificate is displayed

Figure 3-8 : Sequence Diagram

The process begins when the administrator logs into the system, uploads papers, and enters student information into the web interface in order to make a new submission.

When the payment is completed, the web forwards the request to the block chain. It creates the IPFS CID, emails it to the student, and stores the data inside the blockchain.

The student gives the CID to the other university for verification when they pursue higher education.

Another university will log in to the online interface using the cid for verification. Web will send the request query to blockchain for validation. Blockchain will deliver the request's outcome.

Following verification, the university will want to view the certificate.

3.8 Methodology

For Methodology we opted for Agile Methodology.The Agile methodology is a project management approach that involves breaking the project into phases and emphasizes continuous collaboration and improvement. Teams follow a cycle of planning, executing, and evaluating.

We divided the methodology into 2 parts.
First part is the Architectural Phase and the second part is the Development phase. The project outlines all the processes followed to come up with the software that is from analysis to testing the system. Also, the entire work will be divided amongst the entire team so that all the features can be worked upon.
The COS,POS ,PSOS for CMPN will be done as per guidelines from Mumbai university.

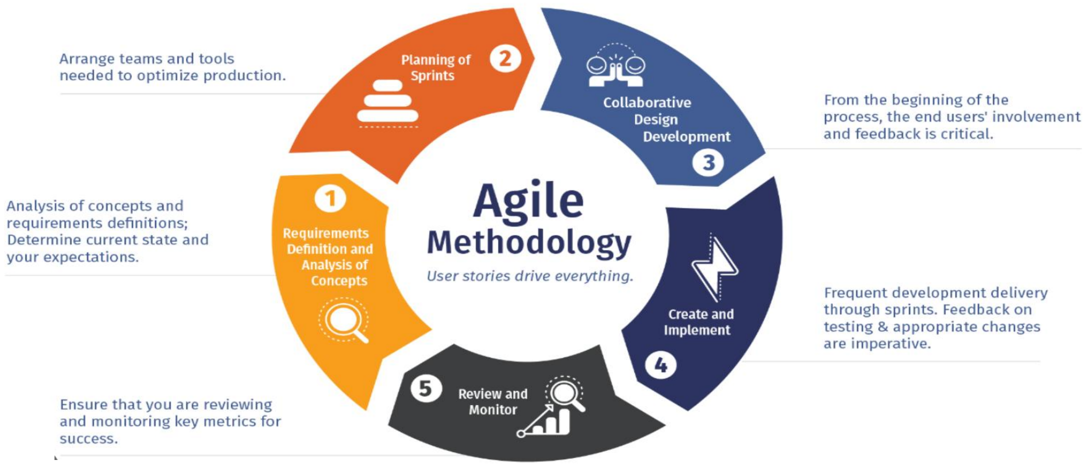

Arrange teams and tools needed to optimize production.
Planning of Sprints
2
Collaborative Design Development
3
From the beginning of the process, the end users' involvement and feedback is critical.
Analysis of concepts and requirements definitions; Determine current state and your expectations.
1
Requirements Definition and Analysis of Concepts
Agile Methodology
User stories drive everything.
Create and Implement
4
Frequent development delivery through sprints. Feedback on testing & appropriate changes are imperative.
5
Review and Monitor
Ensure that you are reviewing and monitoring key metrics for success.

Figure 3-9 : Agile Methodology

1. Initiation and Requirement Gathering

Identify key requirements through stakeholder input, focusing on document storage, security, and verification. Develop user stories and prioritize the backlog based on business needs.

2. Planning

Define sprint goals and plan the roadmap, with a focus on delivering incremental value. Create a sprint backlog with tasks for each development cycle.

3. Development

Implement features in short sprints, collaborating across cross-functional teams. Conduct daily stand-ups to track progress and resolve issues, with regular code reviews and pair programming.

4. Testing and Quality Assurance

Perform unit, integration, and system testing to validate functionality. Conduct GUI testing for usability and user acceptance testing (UAT) to ensure the system meets expectations.

5. Review and Retrospective

Conduct sprint reviews to gather feedback and retrospectives to identify areas for improvement. Use insights to adjust the development approach and plan future sprints.

6. Deployment and Maintenance

Deploy the system to production, monitor performance, and provide ongoing support. Implement a maintenance plan for continuous improvement, and adjust based on feedback and evolving requirements.

This concise approach ensures an adaptable development process with a focus on iterative progress, stakeholder feedback, and collaborative teamwork, leading to a successful blockchain-based system for educational record storage and authentication.

3.9 Implementation Plan

Planning and Design: Developing a decentralized file system with Blockchain, Pinata, IPFS, Solidity programming for smart contracts, and Metamask involves several distinct steps that result in a seamlessly integrated system. The process begins with careful planning and design, in which the project's objectives and requirements are defined. This phase also entails defining the structure of the smart contracts and their interactions with IPFS and Pinata, as well as determining user roles in the system.

Development of Solidity Smart Contracts: The core logic for file operations and interactions with IPFS is encapsulated within Solidity Smart Contracts. Key functions are defined to handle file uploading, retrieval, and management while ensuring data integrity and security.

Setting up an IPFS Node: An IPFS node is established to host and retrieve files in a distributed manner. Understanding Content Identifiers (CIDs) is crucial for locating and retrieving files on the IPFS network.

Integration of Pinata: Pinata, a user-friendly IPFS service, is integrated into the system for robust file management. Users sign up for Pinata accounts and generate API keys to enable interactions with Pinata's services.

Smart Contract Deployment: Solidity contracts are compiled into bytecode and deployed onto a suitable blockchain network, such as Ethereum. Funding the contract with cryptocurrency facilitates interactions within the decentralized ecosystem.

User Interface (UI) Development: A user-friendly UI, typically a web application, is developed to enable user interaction. Users connect their wallets, often through Metamask, to the dApp, allowing them to initiate transactions and perform file operations.

File Upload and Retrieval: Users initiate file upload and retrieval through the UI, triggering interactions with smart contracts. Smart contracts interact with IPFS and Pinata to store files and metadata for uploading and retrieving files for users.

Testing and Optimization: Rigorous testing and optimization are conducted to ensure functionality, security, and efficiency. Smart contracts and UI interactions are fine-tuned to minimize gas fees and enhance the user experience.

4 Implementation

4.1 Introduction

In this section, we delineate the implementation blueprint for our blockchain-based transcript verification system. Following exhaustive analysis and design phases, we are poised to translate our vision into a robust, decentralized solution that revolutionizes the authentication of academic credentials.

Contextualization: The genesis of our endeavor lies in addressing the pervasive challenges plaguing traditional transcript verification systems. Instances of credential fraud, cumbersome verification processes, and the lack of a unified, tamper-proof repository underscore the pressing need for innovation. By leveraging blockchain technology, we endeavor to establish a transparent, immutable ledger for academic transcripts, mitigating fraud and enhancing trust in credential verification processes.

Summary of Preceding Sections: Our journey commenced with a comprehensive examination of existing verification systems, elucidating their limitations and shortcomings. Through meticulous research and stakeholder consultations, we formulated a strategic blueprint for our blockchain solution. Key decisions, including the choice of blockchain platform, consensus mechanism, and data schema, were informed by this analysis, laying a sturdy foundation for implementation.

Outline of the Implementation Plan: The implementation of our blockchain-based transcript verification system unfolds in iterative stages, each meticulously crafted to ensure seamless integration and optimal functionality. The roadmap encompasses the development of smart contracts for transcript issuance and verification, the establishment of a decentralized network of nodes for consensus, and the creation of user-friendly interfaces for stakeholders. Additionally, stringent security measures, such as cryptographic hashing and permissioned access controls, will safeguard the integrity and confidentiality of academic records.

Setting Expectations: Throughout this section, we delve into the intricate details of each implementation phase, elucidating the technological components, deployment strategies, and anticipated outcomes. By the conclusion of this exposition, readers will gain a comprehensive understanding of our implementation strategy and the transformative potential of our blockchain-based transcript verification system.

4.2 Implementation of Front end

This section presents a detailed overview of the front-end implementation for our project developed using React, a popular JavaScript library for building user interfaces. Through the convergence of innovative design principles and cutting-edge development methodologies, our endeavor seeks to deliver a seamless and immersive user experience while ensuring scalability and maintainability.

Front End consists of a simple interface that allows users to navigate through the website, mainly for login, registration and interacting with solidity backend and MongoDb server efficiently.

4.3 Implementation of Backend

For Backend we have used :

Pseudo code: For Admin:

```
// Admin enters credentials
credentialsForm = displayForm() // Display a form for the admin to enter credentials
pdfFile = credentialsForm.uploadPDF() // Uploads a PDF file of minimum 10MB
studentEmail = credentialsForm.getEmail() // Admin enters student email
studentName = credentialsForm.getName() // Admin enters student name

// Payment process through Metamask
paymentStatus = metamaskPayment() // Initiate payment process through Metamask
if paymentStatus == approved:
    // Generate CID and store in IPFS
    cid = generateCID(pdfFile) // Generate CID for the uploaded PDF file
    ipfsStore(cid, pdfFile) // Store PDF file in IPFS with generated CID

    // Send CID through email
sendEmail(studentEmail, "Your CID", cid) // Send generated CID to student's email
```

Pseudo code:For verifier:

```
// Verifier verifies CID
function verifyCID(cid, studentName, verifierName, organizationName):
  if cidExistsInIPFS(cid):
    // Open document
     document = openDocument(cid) // Retrieve document associated with CID from IPFS
    displayDocument(document) // Display the document to the verifier
    logVerification(cid, studentName, verifierName, organizationName, "Verified") // Log verification status
    return "Document opened"
  else:
    return "Credentials not found"
```

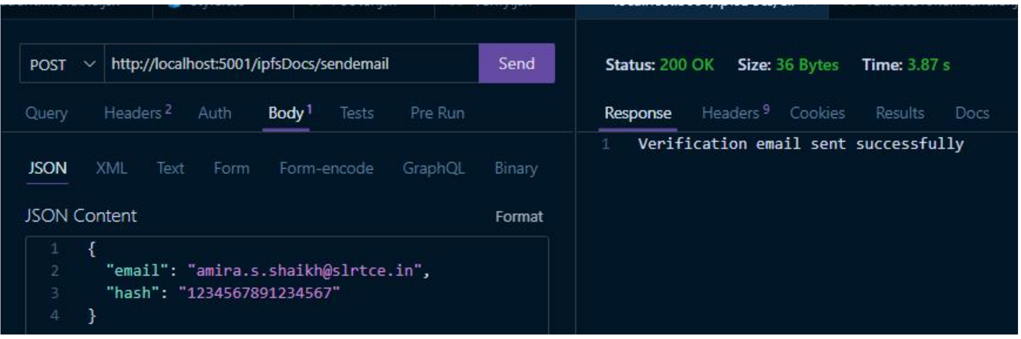
SOLIDITY CODE:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract IPFSHashStorage {
  mapping(string => bool) public ipfsHashes;

  event HashStored(string indexed hash);

  function storeHash(string memory _cid) external {
    string memory hash = _cid;
    ipfsHashes[hash] = true;
    emit HashStored(hash);
  }
  function hashExists(string memory _hash) external view returns (bool) {
    return ipfsHashes[_hash];
  }
}
```

4.4 Implementation of API

We have used RestAPI to provide an interface between the model(database) and controller (API).

We have used three endpoints, which are used to store files in IPFS, store CID in blockchain and server database capturing transactions.



http://localhost:5001/ipfsDocs/sendemail

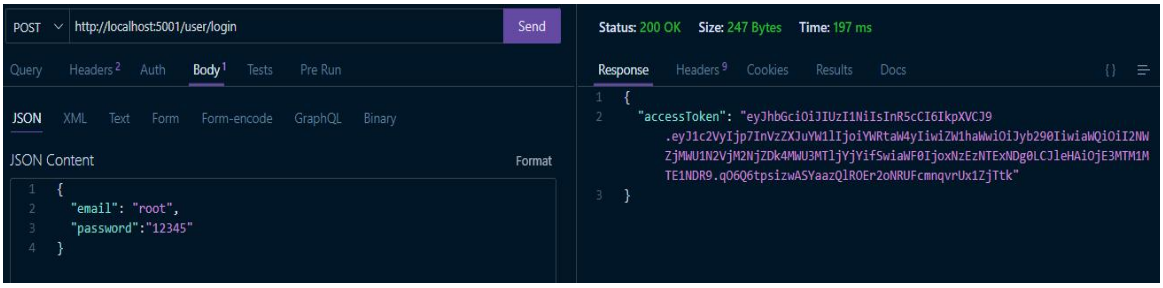
```
{
  "email": "amira.s.shaikh@slrtce.in",
  "hash": "1234567891234567"
}
```

Status: 200 OK Size: 36 Bytes Time: 3.87 s

```
Verification email sent successfully
```

i

Figure 4-1 : Api that sends IPFS CID to student's email.



http://localhost:5001/user/login

```
{
  "email": "root",
  "password":"12345"
}
```

Status: 200 OK Size: 247 Bytes Time: 197 ms

```
{
  "accessToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
     .eyJ1c2VyIjp7InVzZXJuYW1lIjoiYWRtaW4yIiwiZW1haWwiOiJyb290IiwiaWQiOiI2NW
     ZjMWU1N2VjM2NjZDk4MWU3MTljYjYifSwiaWF0IjoxNzEzNTExNDg0LCJleHAiOjE3MTM1M
     TE1NDR9.qO6Q6tpsizwASYaazQlROEr2oNRUFcmnqvrUx1ZjTtk"
}
```

Figure 4-2 : Api for login.

5 Testing

5.1 Introduction

In software development, testing is an essential step that guarantees a system is dependable, safe, and easy to use. Testing has several key goals for a blockchain-based system that stores and verifies student degree information. It finds logical fallacies, security flaws, and coding problems that could compromise the functionality or security of the system. The platform is thoroughly tested for security flaws, including data leaks, unauthorized access, and denial-of-service assaults. These types of attacks are particularly dangerous for systems that hold private student information.

Integration testing ensures that the blockchain, IPFS, smart contracts, and user interfaces all communicate with one other seamlessly by confirming how various components interact. Performance testing evaluates how well the system can manage different loads to make sure it can withstand heavy demand without experiencing a noticeable slowdown in speed or efficiency.

Compliance testing verifies that the system complies with legal and regulatory requirements, particularly those pertaining to data security and the maintenance of educational records.

Because it uses actual users to evaluate the system's usability and overall user experience, user acceptability testing, or UAT, is essential. Verifying that the platform meets user expectations is a crucial stage that enables developers to make the required adjustments based on input from real users.The ultimate goal of testing is to create a dependable, safe, and user-friendly platform that meets the needs of educational institutions, learners, employers, and other pertinent stakeholders. This procedure is essential for both a good launch and long-term success since it fosters trust in the system.

5.2 GUI test

GUI (Graphical User Interface) testing involves evaluating the user interface of an application to ensure it functions correctly, meets design specifications, and provides a smooth user experience. For a blockchain-based system designed to store and verify student degree information, GUI testing ensures that users, including educational institutions, students, and employers, can interact with the system intuitively and without errors.

5.2.1 GUI description

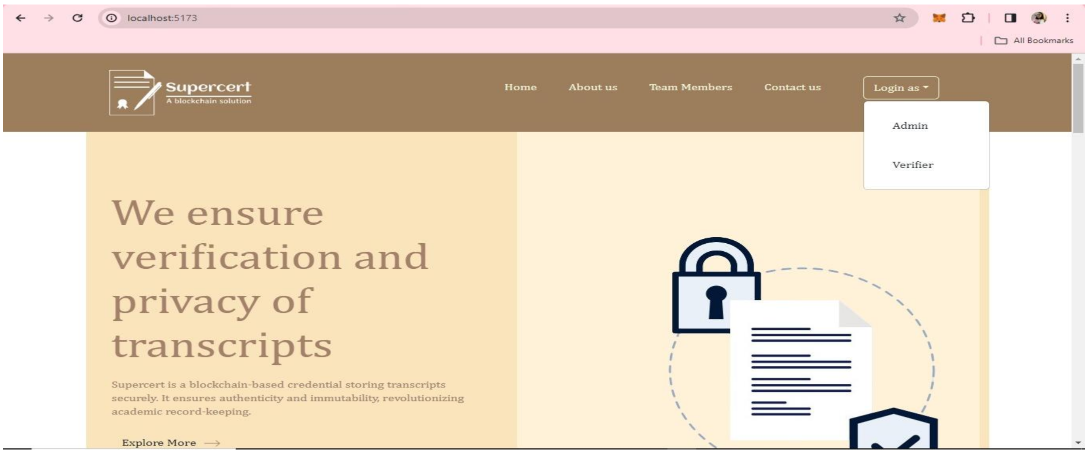
In a blockchain-based system for storing and verifying student degree information, the GUI serves as the primary interface for users like educational institutions, students, employers, and third-party verifiers. Here's how the GUI would typically be structured:

Dashboard: The central hub where users can access different functionalities, such as uploading documents, verifying certificates, and managing admin accounts.

Document Upload: A section where educational institutions can upload student documents like transcripts and certificate. This section may contain file input fields, submit buttons, and status indicators to show upload progress.

Verification Section: Allows users to verify documents by entering unique identifiers or scanning QR codes. This section typically includes text fields for input and display areas for the document's details.

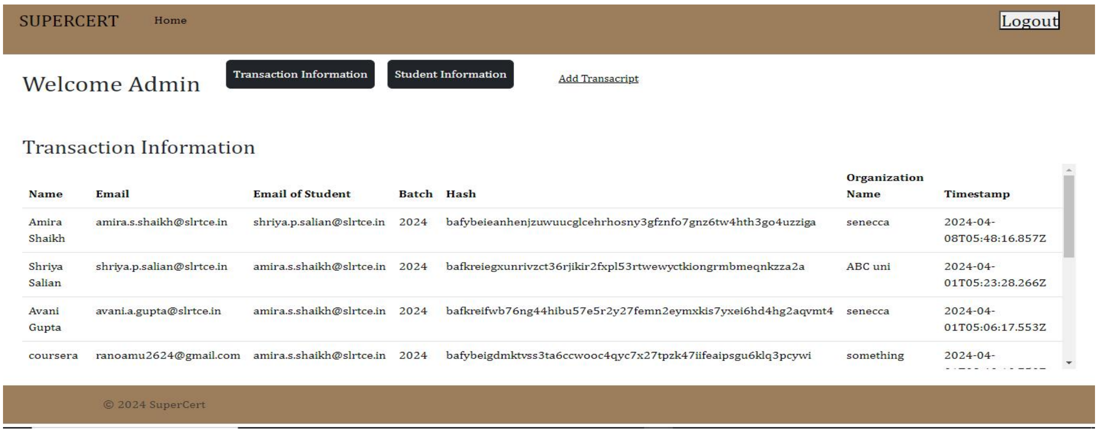
Notifications and Alerts: Pop-up messages or alerts that inform users of important events, such as successful uploads, verification results, or system errors. These notifications provide immediate feedback to users.



We ensure verification and privacy of transcripts

Supercert is a blockchain-based credential storing transcripts securely. It ensures authenticity and immutability, revolutionizing academic record-keeping.

Figure 5-1 : Dashboard.

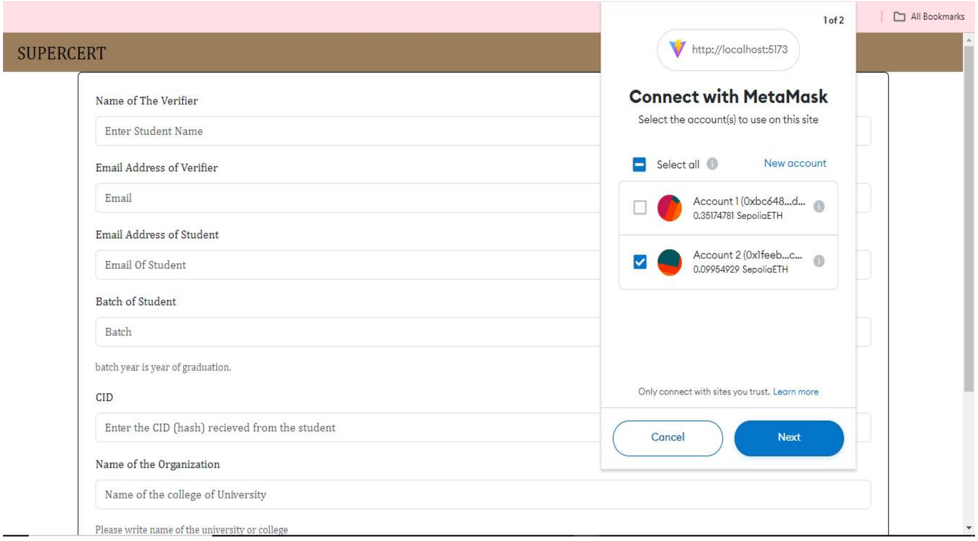


Welcome Admin

Transaction Information

Name	Email	Email of Student	Batch	Hash	Organization Name	Timestamp
Amira Shaikh	amira.s.shaikh@slrtce.in	shriya.p.salian@slrtce.in	2024	bafybeieanhenjzuwuucglcehrhosny3gfznfo7gnz6tw4hth3go4uzziga	senecca	2024-04-08T05:48:16.857Z
Shriya Salian	shriya.p.salian@slrtce.in	amira.s.shaikh@slrtce.in	2024	bafkreiegxunrivzct36rjikir2fxpl53rtwewyctkiongrmbmeqnkzza2a	ABC uni	2024-04-01T05:23:28.266Z
Avani Gupta	avani.a.gupta@slrtce.in	amira.s.shaikh@slrtce.in	2024	bafkreifwb76ng44hibu57e5r2y27femn2eymxkis7yxei6hd4hg2aqvmt4	senecca	2024-04-01T05:06:17.553Z
coursera	ranoamu2624@gmail.com	amira.s.shaikh@slrtce.in	2024	bafybeigdmktvss3ta6ccwooc4qyc7x27tpzk47iifeaipsgu6klq3pcywi	something	2024-04-

Figure 5-2 : Admin Dashboard.



Name of The Verifier

Enter Student Name

Email Address of Verifier

Email

Email Address of Student

Email Of Student

Batch of Student

Batch

batch year is year of graduation.

CID

Enter the CID (hash) recieved from the student

Name of the Organization

Name of the college of University

Please write name of the university or college

Connect with MetaMask

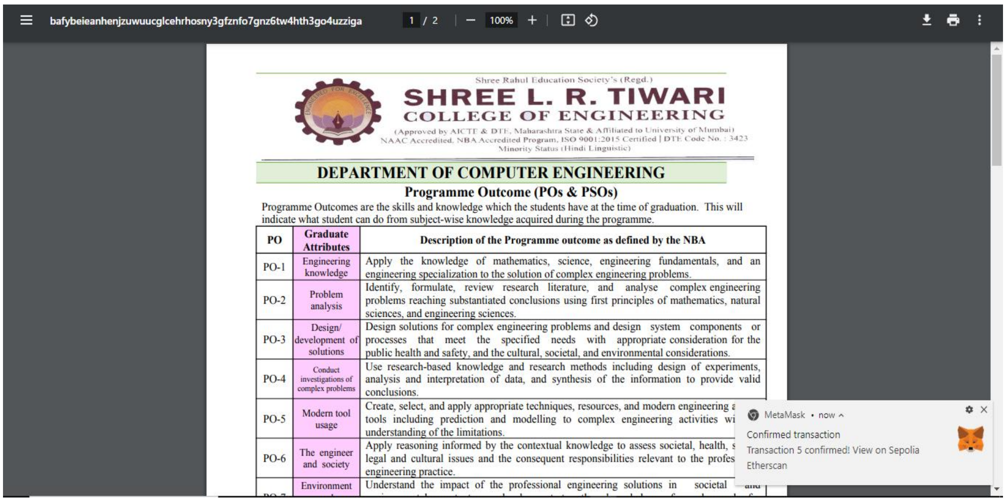
Select the account(s) to use on this site

□ Account 1 (0xbc648...d... 0.35174781 SepoliaETH

☑ Account 2 (0x1feeb...c... 0.09954929 SepoliaETH

Only connect with sites you trust. Learn more

Figure 5-3 : Payment Process.



Shree Rahul Education Society's (Regd.)

SHREE L. R. TIWARI
COLLEGE OF ENGINEERING

(Approved by AICTE & DTE, Maharashtra State & Affiliated to University of Mumbai)
NAAC Accredited, NBA Accredited Program, ISO 9001:2015 Certified | DTE Code No. : 3423
Minority Status (Hindi Linguistic)

DEPARTMENT OF COMPUTER ENGINEERING

Programme Outcome (POs & PSOs)

Programme Outcomes are the skills and knowledge which the students have at the time of graduation. This will indicate what student can do from subject-wise knowledge acquired during the programme.

PO	Graduate Attributes	Description of the Programme outcome as defined by the NBA
PO-1	Engineering knowledge	Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
PO-2	Problem analysis	Identify, formulate, review research literature, and analyse complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO-3	Design/ development of solutions	Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
PO-4	Conduct investigations of complex problems	Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
PO-5	Modern tool usage	Create, select, and apply appropriate techniques, resources, and modern engineering a tools including prediction and modelling to complex engineering activities wi understanding of the limitations.
PO-6	The engineer and society	Apply reasoning informed by the contextual knowledge to assess societal, health, s legal and cultural issues and the consequent responsibilities relevant to the profes engineering practice.
	Environment	Understand the impact of the professional engineering solutions in societal and

MetaMask • now

Confirmed transaction

Transaction 5 confirmed! View on Sepolia Etherscan

Figure 5-4 : Viewing the transcript.

5.2.2 System GUI test plan

This test plan outlines the approach to test the GUI for a block chain-based system designed to store and verify student transcript information. It covers functionality, usability, consistency, compatibility, and accessibility to ensure a user-friendly and error-free interface.

Login and Authentication: Validate the login process, including handling invalid credentials.

Document Upload: Test the process of uploading student documents and handling various file formats.

Document Verification: Ensure users can verify documents using unique identifiers or QR codes.

Notifications and Alerts: Test pop-up messages and alerts for successful operations, errors, and system events.

Navigation and Layout: Validate consistent navigation and layout across the application.

Upload a new transcript – When uploading a new transcript is invoked, following are the test plan. Verify a transcript – When uploading a new transcript, following are the test plan.

Test:

1. Use of Cancel button before making a payment.
2. Provide invalid input or credential.
3. Check whether email is received or not.
4. Check for button navigation.
5. Check if document upload is properly handled.

5.2.3 System GUI test result

1. Tester: Akanksha Gairola akanksha.a.gairola@slrtce.in
2. test date:March 17,2024
3. scope of test: Complete GUI test according to the described test plan.
4. Test environment:The test client was Chrome running under Windows
5. Test log: The test log is presented below:

Case: Use of Cancel button before making a payment.
Action: Click cancel button.
Result: OK,No transcript was not stored in block chain.
Checked: Button worked totally fine.

Case: Check if all elements are working fine even if the screen is reduced
Action: Reduce the size of website.
Result: OK.
Checked: Element were intacted.

Case: Provide invalid credentials.
Action: Enter invaild credentials.
Result: OK.
Checked: Error message popped up, and redirect to dashboard.

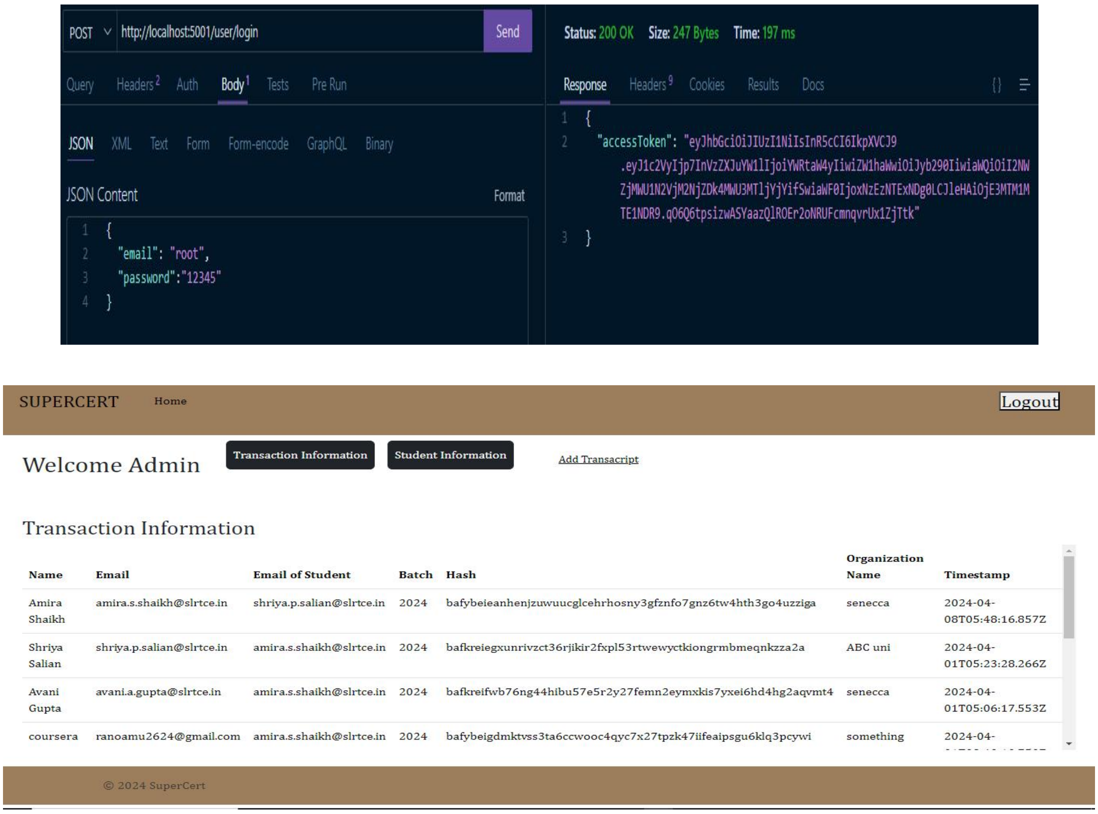
Case: Document upload is properly handled.
Action: Upload document more than 10mb.
Result: OK.
Checked: Error message popped up as uploaded document should be less than 10mb.

6 Result and Discussion

6.1 Introduction

The result of implementing the suggested system demonstrates its usefulness in enabling decentralized file management using blockchain technology. Users may securely upload and retrieve documents by combining services like Pinata and IPFS with smart contracts, ensuring access and data integrity over time. The deployment of smart contracts on blockchain networks like Ethereum enables seamless interactions within the decentralized ecosystem, which is powered by cryptocurrency transactions. The system was able to work perfectly fine and generated expected output to the user.

6.2 Result on Case 1



```
http://localhost:5001/user/login
```

```
{
  "email": "root",
  "password":"12345"
}
```

Status: 200 OK   Size: 247 Bytes   Time: 197 ms

```
{
  "accessToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
     .eyJ1c2VyIjp7InVzZXJuYW1lIjoiYWRtaW4yIiwiZW1haWwiOiJyb290IiwiaWQiOiI2NW
     ZjMWU1N2VjM2NjZDk4MWU3MTljYjYifSwiaWF0IjoxNzEzNTExNDg0LCJleHAiOjE3MTM1M
     TE1NDR9.qO6Q6tpsizwASYaazQlROEr2oNRUFcmnqvrUx1ZjTtk"
}
```

Welcome Admin

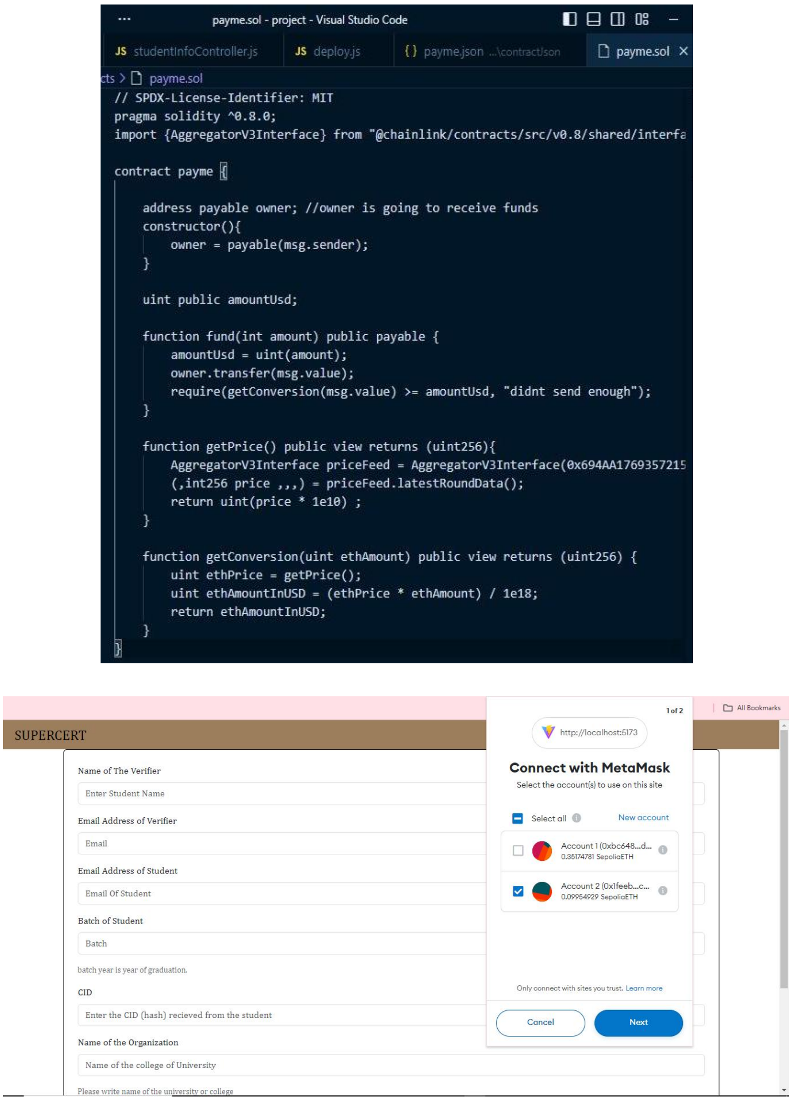
Transaction Information

Name	Email	Email of Student	Batch	Hash	Organization Name	Timestamp
Amira Shaikh	amira.s.shaikh@slrtce.in	shriya.p.salian@slrtce.in	2024	bafybeieanhenjzuwuucglcehrhosny3gfznfo7gnz6tw4hth3go4uzziga	senecca	2024-04-08T05:48:16.857Z
Shriya Salian	shriya.p.salian@slrtce.in	amira.s.shaikh@slrtce.in	2024	bafkreiegxunrivzct36rjikir2fxpl53rtwewyctkiongrmbmeqnkzza2a	ABC uni	2024-04-01T05:23:28.266Z
Avani Gupta	avani.a.gupta@slrtce.in	amira.s.shaikh@slrtce.in	2024	bafkreifwb76ng44hibu57e5r2y27femn2eymxkis7yxei6hd4hg2aqvmt4	senecca	2024-04-01T05:06:17.553Z
coursera	ranoamu2624@gmail.com	amira.s.shaikh@slrtce.in	2024	bafybeigdmktvss3ta6ccwooc4qyc7x27tpzk47iifeaipsgu6klq3pcywi	something	2024-04-

Figure 6-1:Connection of Admin dashboard with API.

The image shows the screenshot of successful connection between API and UI. Above picture is the Login API where the email and password is define. When the admin connect with the database, and enters the login credentials. Admin Dashboard gets log in without any issue , and all the element works fine.

6.3 Result of Case 2


payme.sol - project - Visual Studio Code
JS studentInfoController.js
JS deploy.js
{} payme.json ...\contractJson
payme.sol
cts > payme.sol

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
import {AggregatorV3Interface} from "@chainlink/contracts/src/v0.8/shared/interfa

contract payme {

    address payable owner; //owner is going to receive funds
    constructor(){
        owner = payable(msg.sender);
    }

    uint public amountUsd;

    function fund(int amount) public payable {
        amountUsd = uint(amount);
        owner.transfer(msg.value);
        require(getConversion(msg.value) >= amountUsd, "didnt send enough");
    }

    function getPrice() public view returns (uint256){
        AggregatorV3Interface priceFeed = AggregatorV3Interface(0x694AA1769357215
        (,int256 price ,,,) = priceFeed.latestRoundData();
        return uint(price * 1e10) ;
    }

    function getConversion(uint ethAmount) public view returns (uint256) {
        uint ethPrice = getPrice();
        uint ethAmountInUSD = (ethPrice * ethAmount) / 1e18;
        return ethAmountInUSD;
    }
}
```

Name of The Verifier

Enter Student Name

Email Address of Verifier

Email

Email Address of Student

Email Of Student

Batch of Student

Batch

batch year is year of graduation.

CID

Enter the CID (hash) recieved from the student

Name of the Organization

Name of the college of University

Please write name of the university or college

Connect with MetaMask

Select the account(s) to use on this site

☐ Select all

New account

☐ Account 1 (0xbc648...d... 0.35174781 SepoliaETH

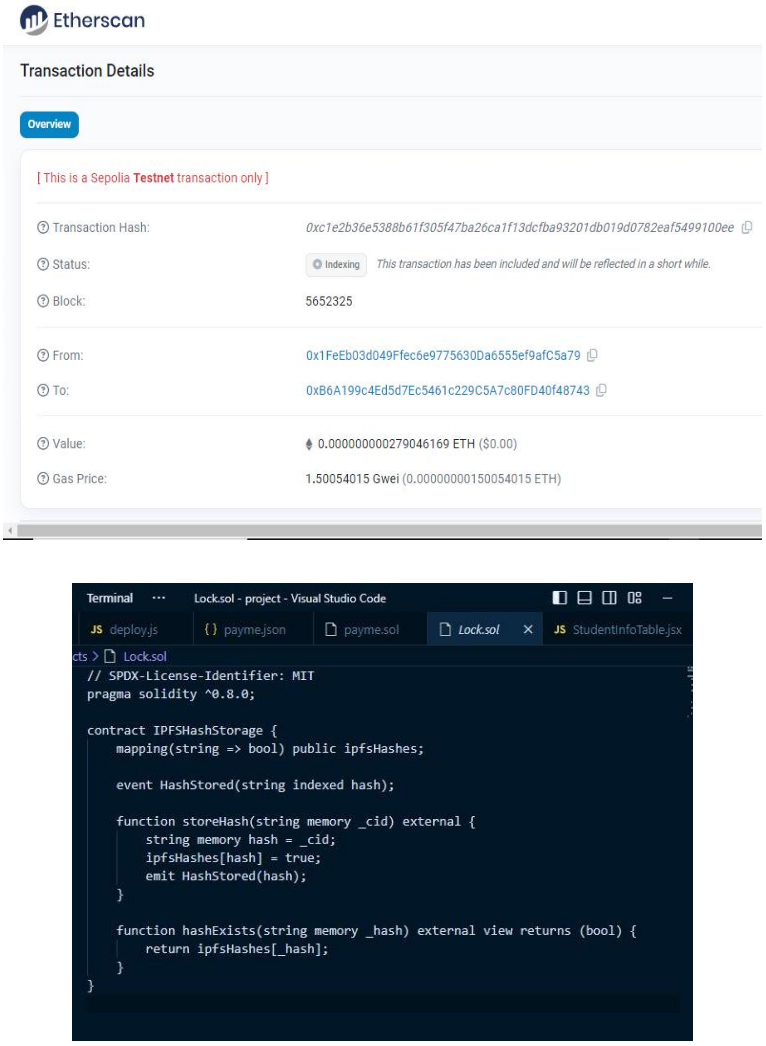
☑ Account 2 (0x1feeb...c... 0.09954929 SepoliaETH

Only connect with sites you trust. Learn more

Figure 6-2:Connection of Smart Contract and payment model.

The image shows the screenshot of successful implement Smart contract for payment. Payment model works perfectly fine. Above picture is Smart Contract where all the functionality of the payment is defined.

6.4 Result of Case 3



Transaction Details

[This is a Sepolia **Testnet** transaction only]

Transaction Hash: *0xc1e2b36e5388b61f305f47ba26ca1f13dcfba93201db019d0782eaf5499100ee*

Status: Indexing *This transaction has been included and will be reflected in a short while.*

Block: 5652325

From: 0x1FeEb03d049Ffec6e9775630Da6555ef9afC5a79

To: 0xB6A199c4Ed5d7Ec5461c229C5A7c80FD40f48743

Value: 0.000000000279046169 ETH ($0.00)

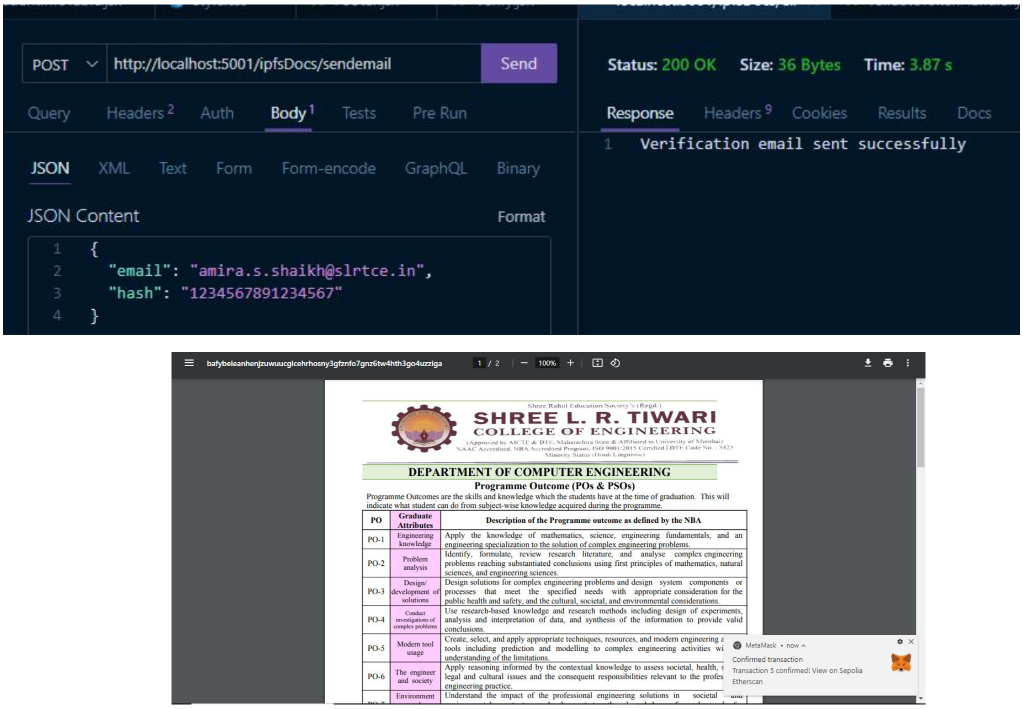
Gas Price: 1.50054015 Gwei (0.00000000150054015 ETH)

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract IPFSHashStorage {
    mapping(string => bool) public ipfsHashes;

    event HashStored(string indexed hash);

    function storeHash(string memory _cid) external {
        string memory hash = _cid;
        ipfsHashes[hash] = true;
        emit HashStored(hash);
    }

    function hashExists(string memory _hash) external view returns (bool) {
        return ipfsHashes[_hash];
    }
}
```

Figure 6-3: Smart Contract and transaction details.

When a transaction is made the contract is checks for the hash if it is already present in blockchain else it will store the IPFS Hash in blockchain and transaction details can be seen.

6.5 Result of Case 4



```
{
  "email": "amira.s.shaikh@slrtce.in",
  "hash": "1234567891234567"
}
```

Status: 200 OK Size: 36 Bytes Time: 3.87 s

```
Verification email sent successfully
```

Shree Rahul Education Society's (Regd.)

SHREE L. R. TIWARI
COLLEGE OF ENGINEERING

(Approved by AICTE & DTE, Maharashtra State & Affiliated to University of Mumbai)
NAAC Accredited, NBA Accredited Program, ISO 9001:2015 Certified | DTE Code No. : 3423
Minority Status (Hindi Linguistic)

DEPARTMENT OF COMPUTER ENGINEERING

Programme Outcome (POs & PSOs)

Programme Outcomes are the skills and knowledge which the students have at the time of graduation. This will indicate what student can do from subject-wise knowledge acquired during the programme.

PO	Graduate Attributes	Description of the Programme outcome as defined by the NBA
PO-1	Engineering knowledge	Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
PO-2	Problem analysis	Identify, formulate, review research literature, and analyse complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO-3	Design/ development of solutions	Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
PO-4	Conduct investigations of complex problems	Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
PO-5	Modern tool usage	Create, select, and apply appropriate techniques, resources, and modern engineering a tools including prediction and modelling to complex engineering activities wi understanding of the limitations.
PO-6	The engineer and society	Apply reasoning informed by the contextual knowledge to assess societal, health, s legal and cultural issues and the consequent responsibilities relevant to the profes engineering practice.
	Environment	Understand the impact of the professional engineering solutions in societal and

MetaMask • now

Confirmed transaction

Transaction 5 confirmed! View on Sepolia Etherscan

*Figure 6-4: **Result of after-payment output .***

From send mail api, mail is send to repected student.

After the payment is done we can see the certificate or transcript of the student.

7 Conclusion and Future work.

In conclusion, SuperCert represents an advanced and innovative solution for addressing the challenges associated with educational certificates, such as fraud, verification, and data security. Certificates recorded on the blockchain become tamper-proof and can be easily verified by educational institutions and employers. The system incorporates robust identity verification processes to validate the identity of applicants, making it difficult for fraudulent individuals to exploit the system. Data security is a top priority, and SuperCert employs encryption and secure storage mechanisms to protect sensitive user information and certificates. The use of blockchain technology enhances transparency in the certification process, fostering trust among educational institutions. By automating the certificate verification process and reducing the administrative burden on educational institutions, SuperCert improves efficiency in the educational certification ecosystem.

The future scopes include working with universities and educational institutions to establish blockchain-based credential verification systems on a larger scale. This might include standardizing the process across numerous colleges and leveraging blockchain technology into current student databases. In addition to educational credentials, blockchain technology can be used to verify professional qualifications, licenses, and legal documents. Exploring the expansion of blockchain verification to these domains could boost trust and transparency across sectors. Constantly upgrading security procedures inside blockchain systems would be required to protect against cyber threats and preserve the integrity of stored certificates. This may include investigating advanced encryption techniques, multi-factor authentication, and biometric verification methods. Promoting widespread use of blockchain-based certificate verification systems on a worldwide scale. This could include raising awareness, offering training and support, and addressing regulatory issues to make implementation easier across multiple countries and jurisdictions. Interoperability, refers to the development of standards and protocols that enable different blockchain networks and systems to communicate with each other. This will enable the easy interchange and verification of certificates across several systems, increasing efficiency and usefulness.

8 References

[1] Bessa, Emanuel E., and Joberto SB Martins. "A blockchain-based educational record repository." arXiv preprint arXiv:1904.00315 (2019).

[2] Rustemi, Avni, et al. "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification." IEEE Access (2023).

[3] K. B. Dubey and M. Goyal, ‘‘Smart certificate using blockchain,’’ J. Comput. Sci.,vol. 18, no. 9, pp. 877–884, Sep. 2022, doi: 10.3844/jcssp.2022.877.884.

[4] San, A. M., Chotikakamthorn, N., & Sathitwiriyawong, C. (2019). Blockchain-based Learning Credential Verification System with Recipient Privacy Control. 2019 IEEE International Conference on Engineering, Technology and Education (TALE).doi:10.1109/tale48000.2019.9225878.

[5] Q. Tang, ‘‘Towards using blockchain technology to prevent diploma fraud,’’ IEEE Access,vol. 9, pp. 168678–168688, 2021, doi: 10.1109/ACCESS.2021.313790.

[6] Pathak, Shivani, et al. "Blockchain-based academic certificate verification system—a review." Advanced Computing and Intelligent Technologies: Proceedings of ICACIT 2022 (2022): 527-539..

[7] Bele, Roshani S., and Jayant P. Mehare. "A review on digital degree certificates using blockchain technology." IJCRT 9.2 (2021): 2320-2882.

[8] Samanta, A.K., Sarkar, B.B. & Chaki, N. A Blockchain-Based Smart Contract Towards Developing Secured University Examination System. J. of Data, Inf. and Manag. 3, 237–249 (2021). https://doi.org/10.1007/s42488-021-00056-0.

[9] Meirobie, Isyak, et al. "Framework Authentication e-document using Blockchain Technology on the Government system." International Journal of Artificial Intelligence Research 6.2 (2022).

[10] Shakan, Yassynzhan, et al. "Verification of university student and graduate data using blockchain technology." International Journal of Computers Communications & Control 16.5 (2021).

[11] ONWUASOANYA, NC, and BE EZE. "MYTRANSCRIPT: AN ACADEMIC TRANSCRIPT DECENTRALISED WEB APPLICATION SYSTEM BASED ON THE ETHEREUM BLOCKCHAIN." (2022).

[12] Imam, Iftekher Toufique, et al. "DOC-BLOCK: A blockchain based authentication system for digital documents." 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). IEEE, 2021.

[13] Das, Moumita, et al. "A blockchain-based integrated document management framework for construction applications." Automation in Construction 133 (2022): 104001.

[14] Soares, Pamella, et al. "Extending the Docstone to Enable a Blockchain-based Service for Customizable Assets and Blockchain Types." Journal of Software Engineering Research and Development 11.1 (2023): 15-1.

[15] Kuonen, David. "The process of creating, testing, and deploying smart contracts on the Ethereum blockchain using Solidity." (2023).

[16] Mohanty, Debasis, et al. "Blockchain interoperability: Towards a sustainable payment system." Sustainability 14.2 (2022): 913.

[17] Enwerem, Udochukwu C. "BLOCKCHAIN RESULT AND TRANSCRIPT MANAGEMENT SYSTEM: A CASE STUDY OF FEDERAL UNIVERSITY OF TECHNOLOGY OWERRI." International Conference on Communication and E-Systems For Economic Stability| CeSES. 2023.

[18] Hujare, Ankush R., et al. "DECENTRALIZED FILE SYSTEM USING BLOCKCHAIN."

[19] Singh, Akanksha, Harsh Vardhan Gupta, and Vaishnavi Gupta. "Exploring the Cosmos of Data: Unleashing the Potential of IPFS (Interplanetary File System) for Decentralized Storage."

[20] Alizadeh, Morteza, Karl Andersson, and Olov Schelén. "Efficient decentralized data storage based on public blockchain and IPFS." 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). IEEE, 2020.

[21] Trautwein, Dennis, et al. "Design and evaluation of IPFS: a storage layer for the decentralized web." Proceedings of the ACM SIGCOMM 2022 Conference. 2022.

[22] Doan, Trinh Viet, et al. "Toward decentralized cloud storage with IPFS: opportunities, challenges, and future considerations." IEEE Internet Computing 26.6 (2022): 7-15.

[23] Raghavender, K. V., et al. "Decentralized Smart Contract Certificate System Using Ethereum Blockchain Technology." Second International Conference on Emerging Trends in Engineering (ICETE 2023). Atlantis Press, 2023.

[24] Chaniago, Nero, Parman Sukarno, and Aulia Arif Wardana. "Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain." Register 7.2 (2021): 149-163.

[25] Saleh, Omar S., Osman Ghazali, and Muhammad Ehsan Rana. "Blockchain based framework for educational certificates verification." Journal of critical reviews (2020).

9 Annexure – Published Paper

This topic has been published in “International Journal of Scientific Research in Computer Science, Engineering and Information Technology”

IJSRCSEIT|ISSN: 2456-3307 [Volume 10, Issue 2, March-April-2024, Date of Publication: 18-03-2024, *UGC Approved Journal No:* 64718]

International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT2410266

SuperCert - An Anti-Fraud Identity Intelligence Blockchain Solution for Educational Certificates

Akanksha Gairola[1], Amira Shaikh[1], Shriya Salian[1], Shankar Malve[1],Mr. Pravin Jangid[2]

[1]Student, Computer Engineering Department, Shree LR Tiwari College of Engineering, Mira Road, Mumbai, Maharashtra, India

[2]Assistant Professor, Computer Engineering Department, Shree LR Tiwari College of Engineering, Mira Road, Mumbai, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 10 April 2024

Published: 18 April 2024

Publication Issue

Volume 10, Issue 2

March-April-2024

Page Number

541-550

ABSTRACT

In recent years, the proliferation of fraudulent educational certificates has posed significant challenges to academic institutions, employers, and individuals alike. Such certificates not only undermine the credibility of educational achievements but also jeopardize the integrity of various industries. To combat this issue, this research introduces SuperCert, an innovative anti-fraud identity intelligence blockchain solution tailored for educational certificates. SuperCert leverages blockchain technology to establish a decentralized, immutable ledger that securely stores educational credentials. The system incorporates smart contract functionality to automate verification processes, thereby reducing administrative overhead and enhancing efficiency.

Keywords : Transcript, Verification, Authentication, Confidentiality, Blockchain, Smart Contract, IPFS, Ethereum, Metamask, University.

I. INTRODUCTION

In today's increasingly digital and interconnected world, the validity and authenticity of educational certificates have become paramount. Traditional methods of certificate verification, relying on manual processes and centralized databases, have proven inadequate in addressing the growing sophistication of fraudsters. Falsified documents, altered credentials, and identity theft continue to plague educational institutions, employers, and individuals, leading to widespread distrust and inefficiencies in the verification process. To combat this pervasive issue, this research introduces SuperCert, an innovative anti-fraud identity intelligence blockchain solution specifically designed for educational certificates. SuperCert harnesses the power of blockchain technology, which offers a decentralized, immutable ledger capable of securely recording and verifying transactions. SuperCert incorporates smart contract functionality, enabling automated verification processes and reducing the administrative burden on educational institutions and employers. SuperCert incorporates smart contract functionality, enabling automated verification processes and reducing the administrative burden on educational institutions and employers. Ultimately, this research contributes to the ongoing discourse on blockchain-based solutions for identity management and underscores the transformative potential of SuperCert in ensuring the integrity of educational certificates in the digital age.

II. BACKGROUND

Hard copies of student transcripts were traditionally kept in secure locations, such as a school's academic department or registrar's office. The problem occurs when students pursue further education and the institution needs to verify the transcript they have been given. The difficulty with the certificate for validation is its size; occasionally, the data can get lost or changed. The validator finds it challenging to validate every certificate. With the development of technology, forging fake certifications is simpler. Differentiating between real and fake credentials takes a lot of effort and time. Because of centralization and digitization, the problem of fake credentials has become a nuisance for organizations and recruitment firms alike. Because of centralization and digitization, the problem of fake credentials has become a nuisance for organizations and recruitment firms alike. Innocent people could lose their lives as a result of fake medical care provided by counterfeit doctors and fraudulent structures created by fraudulent engineers.Even the institute engages in time-consuming collaboration with colleges and universities.

III. PROBLEM STATEMENT

The development of a blockchain application that enables educational institutions to preserve immutable transcript records for their students necessitates the creation of an accessible user interface for administrators and students alike. After courses are finished or academic milestones are reached, administrators enter relevant data into the application, which generates digital transcripts that are time-stamped and cryptographically signed. Together with their cryptographic signatures, these transcripts are securely stored on a blockchain network, ensuring transparency and immutability. Afterwards, by obtaining access to the blockchain and confirming the veracity of transcripts, corporations can view comprehensive academic records with cryptographic proof of integrity. Data security and privacy are given top priority by the program through the use of robust encryption and access controls.Scalability and interoperability are important considerations since they can handle various data volumes and interact with existing academic systems with ease. Ongoing technical support and maintenance ensure smooth operation, maximizing adoption and usefulness. All things considered, this blockchain application assists students and companies who verify educational qualifications by enhancing the security, transparency, and dependability of academic information. The current methods are functional, but since the process often takes several weeks, efficiency and security need to be increased. This is costly and environmentally damaging, in addition to being inconvenient and time-consuming.

The solution to this problem is to recognize fake certificates, store certificates, and streamline the internal verification process of an organization's certificates without using a third party.

IV. RELATED WORK

The possibilities of blockchain technology outside of cryptocurrency have attracted a lot of interest lately, especially in the field of education. A number of topics have been studied by academics, such as secure data sharing frameworks, smart contracts for record verification, and decentralized credentialing systems. Initiatives like the Blockchain-based Educational Record Repository (BcER2) [1], which build upon this fundamental research, provide workable options for securely organizing and disseminating educational records. BcER2 promises to transform educational record management by enabling the easy transfer, sharing, and distribution of e-diplomas and e-certificates among professionals in academia and business. This is achieved by utilizing blockchain's intrinsic qualities of authenticity and immutability.

The principles and uses of blockchain technology in a variety of fields, especially education,. Blockchain is still underutilized in supply chain management, banking, insurance, healthcare, and electronic voting, despite its global recognition. It highlights how blockchain has the ability to revolutionize traditional credentialing procedures by highlighting its decentralized structure and unmatched security. The study creates a blockchain certificate system by utilizing Ethereum's platform and the Ethereum Virtual Machine (EVM). [2] This ensures tamper-proof verification through the creation of blocks and distinct hash codes. To maximize blockchain functionality, several consensus methods are used, including Proof of Work (PoW), Proof of Stake (PoS), and Proof of Capacity (PoC). To guarantee the integrity of digital diplomas, the suggested authentication technique makes use of blockchain APIs for transaction validation and verification as well as issuance applications. In general, the research highlights blockchain's role in revolutionizing transparency, expediting verification processes, and fostering trust in the educational ecosystem.

A thorough analysis of blockchain-based digital degree certificate verification. It highlights how important it is to have a decentralized application to effectively handle counterfeit issues, especially considering how many students in India graduate each year. The suggested system seeks to offer verifiable digital certificates with anti-counterfeit safeguards by utilizing blockchain's immutable feature. The procedure involves creating a paper certificate with a unique code attached to it and then uploading it to a public blockchain for safe verification. With less time and money spent on manual verification techniques, this novel approach aims to expedite certificate verification procedures and provide users with more control over their data. [3] It describes the system's architecture and design.

The security of educational certificate verification processes is enhanced through the use of Hyperledger Fabric to construct a blockchain-based architecture. The suggested system provides advantages such as permissioned access, distinctly recognizable digital certificates, transparent network communication, and effective grievance redressal methods by utilizing Hyperledger's permissioned network capabilities. In general, the study enhances the dependability and security of document verification in the academic field, with consequences for ownership, authorization, privacy, and secrecy. [4]

A system that transforms centralized storage into distributed storage records transactions via a decentralized system rather than a centralized one and allows each node to verify the transaction. For this reason, it can be used to store fingerprints from transcripts and official diploma documents that are made public. In order for contracts like diplomas and transcripts uploaded on the Ethereum blockchain to distribute and produce diploma validation and the authenticity of transcripts with transaction hash, consensus, and compliance with ERC-721 token standardization, [5] smart contracts are required for making contract transactions to Ethereum with programming code.The findings demonstrated that it is simple to verify the authenticity of a sample of five electronic documents in PDF format that were published and secured using Ethereum blockchain technology. Our proposed and developed system accounts for invalid and failure cases by providing the user with the appropriate feedback.

The management, preservation, authentication, and potential for tampering of traditional paper and electronic certificates present issues. Certificates are frequently faked, and the fakes are frequently identical to the real ones. As such, the process of certification and verification needs to be improved immediately. We suggest a project that uses blockchain technology for certificate verification in order to safeguard the problems. The college certificate will be uploaded, and the university will enter the student's roll number first.

It will then be saved on the Interplanetary File System (IPFS) [6] and assigned a distinct hash value. Then, with the roll number and distinct hash value, anybody—student, recruiter, or administrator—can obtain and validate the college certificate. In the event that the produced hash value is lost, certificate validation can also be carried out by supplying the certificate and the student's roll number. This method promises speedier verification of educational diplomas, lower expenses, and increased security.

IPFS is a modular set of data organizing and transfer protocols founded on content addressing and peer-to-peer networking. [8] [9] Because IPFS is open-source, it has a wide range of implementation options. While IPFS has various uses, its primary purpose is to publish data (files, directories, webpages, etc.) in a decentralized manner. The use of IPFS facilitates data storage and sharing on distributed networks.

The study explores the development of a distributed file system (DFS) using Solidity [11], a programming language designed for smart contracts on Ethereum. Its aim is to create a user-friendly application for sharing and managing files using blockchain technology. The methodology includes several components, including the design of a smart contract that defines the rules and functions of file management. Tools like Pinata and MetaMask allow users to effectively interact with the system. Uploaded files are assigned a unique ID and are stored in the InterPlanetary File System (IPFS) and Pinata file hosting. MetaMask emphasizes user participation, but smart contract rules govern the storage and retrieval of final files. The DFS architecture consists of several layers: an intelligent application layer, a network layer that ensures proper distribution of files, a storage layer that uses IPFS storage, and a security layer that uses blockchain technology.

The security themes needed for the blockchain-based verification of educational certificates were found and examined in this study. [20] Furthermore, a blockchain-based framework based on the Hyperledger Fabric Framework is suggested for the verification of educational certificates, with an emphasis on certain issues. The blockchain's security themes of ownership, privacy, confidentiality, authorization, and authentication are necessary for the verification of educational diplomas. Employers will be able to see through authentication that the student is reliable and capable of substantiating their statements about their education. Through authorization, the student will be able to complete duties for which they are legally allowed and with the required permits. Confidentiality and privacy will demonstrate that the information and identity contained in the certificate are safeguarded. The suggested framework will be used and applied to a few chosen educational institutions for subsequent work.

V. PROPOSED SOLUTION

To address the difficulty of storing and authenticating transcripts without a central authority while also providing an immutable record using IPFS and the Ethereum Public Blockchain, this solution allows higher education institutions to use this website to check students' transcripts directly through the website. This contributes to the elimination of third parties/centralized authorities, such as universities and colleges, by leveraging blockchain's immutability to prevent tampering or alteration of educational records once they are recorded on the ledger, as many colleges and universities use their own private servers, resulting in centralization.

Using IPFS, the system may deliver high performance and low latency, making it an ideal solution for file storage and sharing. IPFS generates CIDs (content identifiers, which are labels used to point to stuff in IPFS) that can be used as proof of work for transcripts. SuperCert enables educational institutions to register on SuperCert and securely issue digital certificates upon program completion. A real-time verification system that allows instant validation of certificates by educational institutions, or any third-party verifier which enables decentralized verification by providing direct access to blockchain records, ensuring trustworthiness and transparency.

SuperCert offers a comprehensive solution to combat fraud in educational certificates by leveraging blockchain technology, robust verification mechanisms, anti-fraud measures, and a user-centric approach. Through continuous improvement, SuperCert aims to establish itself as the go-to platform for secure and trustworthy verification of educational credentials.

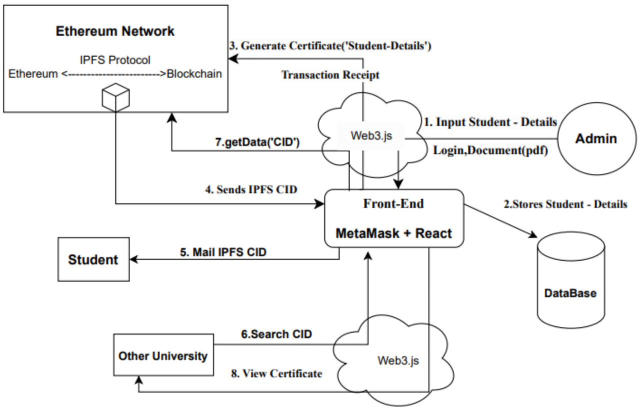


Fig. 1. Data Flow diagram of the Proposed System

Pseudo code: For Admin:

```
// Admin enters credentials
credentialsForm = displayForm() // Display a form for the admin to enter credentials
pdfFile = credentialsForm.uploadPDF() // Admin uploads a PDF file of minimum 10MB
studentEmail = credentialsForm.getEmail() // Admin enters student email
studentName = credentialsForm.getName() // Admin enters student name

// Payment process through Metamask
paymentStatus = metamaskPayment() // Initiate payment process through Metamask
if paymentStatus == approved:
    // Generate CID and store in IPFS
    cid = generateCID(pdfFile) // Generate CID for the uploaded PDF file
    ipfsStore(cid, pdfFile) // Store PDF file in IPFS with generated CID

    // Send CID through email
sendEmail(studentEmail, "Your CID", cid) // Send generated CID to student's email
```

Pseudo code: For verifier:

```
// Verifier verifies CID
function verifyCID(cid, studentName, verifierName, organizationName):
    if cidExistsInIPFS(cid):
        // Open document
        document = openDocument(cid) // Retrieve document associated with CID from IPFS
        displayDocument(document) // Display the document to the verifier
        logVerification(cid, studentName, verifierName, organizationName, "Verified") // Log verification status
        return "Document opened"
    else:
        return "Credentials not found"
```

To understand the proposed solution more clearly, here is the architecture of the system:

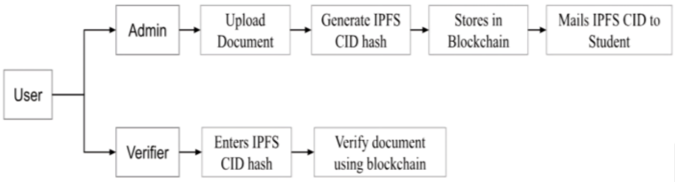


Fig. 2. Architecture of the Proposed System

We have two modules: Admin and Verifier. In this case, the administrator is in charge of uploading students' transcripts and storing them on the blockchain, whilst the verifiers are higher education institutions.

To ensure effective file management, the system utilizes Pinata, an easy-to-use IPFS service. Users create Pinata accounts and generate API keys, allowing their smart contracts to seamlessly connect to Pinata's services. Solidity contracts are compiled into bytecode and then deployed on a suitable blockchain network, such as Ethereum.

Easy to use, typically found in web applications, promotes user participation. Users can begin transactions and perform file operations using the user interface (UI) of the decentralized application (dApp) by connecting their wallets, usually through Metamask. An essential tool in this procedure is the widely used Ethereum wallet plugin, Metamask. Installing Metamask, setting it up to connect to the file system API, and granting the required rights are the steps that users take to ensure safe and verified interactions.

The system is thoroughly tested and makes use of test tokens.

VI. METHODOLOGY

Planning and Design: Developing a decentralized file system with Blockchain, Pinata, IPFS, Solidity programming for smart contracts, and Metamask involves several distinct steps that result in a seamlessly integrated system. The process begins with careful planning and design, in which the project's objectives and requirements are defined. This phase also entails defining the structure of the smart contracts and their interactions with IPFS and Pinata, as well as determine user roles in the system.

Development of Solidity Smart Contracts: The core logic for file operations and interactions with IPFS is encapsulated within Solidity Smart Contracts. Key functions are defined to handle file uploading, retrieval, and management while ensuring data integrity and security.

Setting up an IPFS Node: An IPFS node is established to host and retrieve files in a distributed manner. Understanding Content Identifiers (CIDs) is crucial for locating and retrieving files on the IPFS network.

Integration of Pinata: Pinata, a user-friendly IPFS service, is integrated into the system for robust file management. Users sign up for Pinata accounts and generate API keys to enable interactions with Pinata's services.

Smart Contract Deployment: Solidity contracts are compiled into bytecode and deployed onto a suitable blockchain network, such as Ethereum. Funding the contract with cryptocurrency facilitates interactions within the decentralized ecosystem.

User Interface (UI) Development: A user-friendly UI, typically a web application, is developed to enable user interaction. Users connect their wallets, often through Metamask, to the dApp, allowing them to initiate transactions and perform file operations.

File Upload and Retrieval: Users initiate file upload and retrieval through the UI, triggering interactions with smart contracts. Smart contracts interact with IPFS and Pinata to store files and metadata for uploading and retrieving files for users.

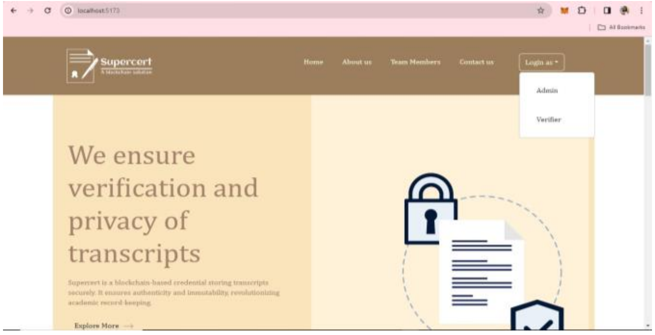
Testing and Optimization: Rigorous testing and optimization are conducted to ensure functionality, security, and efficiency. Smart contracts and UI interactions are fine-tuned to minimize gas fees and enhance the user experience.

VII. RESULTS AND DISCUSSION

The result of implementing the suggested system demonstrates its usefulness in enabling decentralized file management using blockchain technology. Users may securely upload and retrieve documents by combining services like Pinata and IPFS with smart contracts, ensuring access and data integrity over time. The deployment of smart contracts on blockchain networks like Ethereum enables seamless interactions within the decentralized ecosystem, which is powered by cryptocurrency transactions.

Frontend Development:

Develop front-end user interfaces using web technologies (HTML, CSS, JavaScript, and React). Integrating it with Metamask for transaction authentication and signing. Create forms and interfaces for uploading, managing, and sharing files.



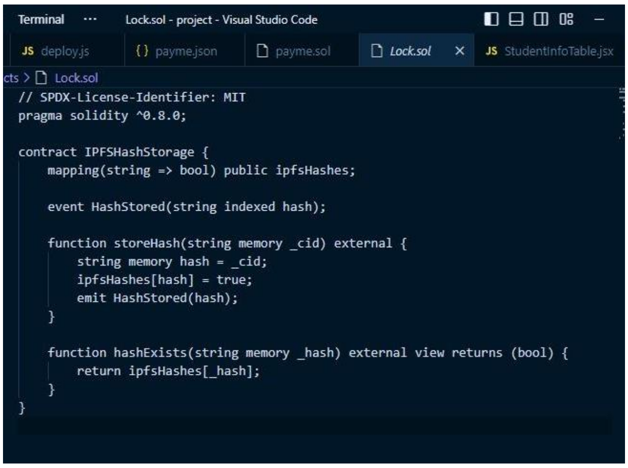
We ensure verification and privacy of transcripts

Supercert is a blockchain-based credential storing transcripts securely. It ensures authenticity and immutability, revolutionizing academic record-keeping.

Fig. 3. Dashboard of SuperCert

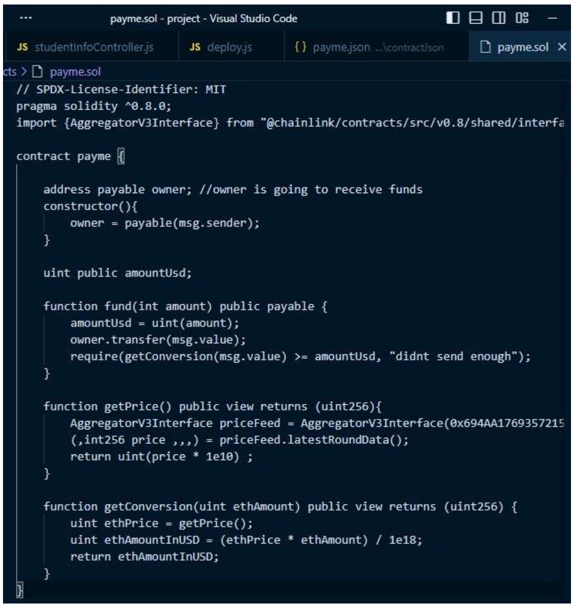
Solidity Smart Contract Development:

Develop smart contracts to store IPFS CID tokens and payments. Create contracts covering storage credentials, access rights, and file metadata management. Defines how files can be loaded, updated, and deleted.



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract IPFSHashStorage {
    mapping(string => bool) public ipfsHashes;

    event HashStored(string indexed hash);

    function storeHash(string memory _cid) external {
        string memory hash = _cid;
        ipfsHashes[hash] = true;
        emit HashStored(hash);
    }

    function hashExists(string memory _hash) external view returns (bool) {
        return ipfsHashes[_hash];
    }
}
```

Fig. 4. Smart Contract For IPFS Hash Storage

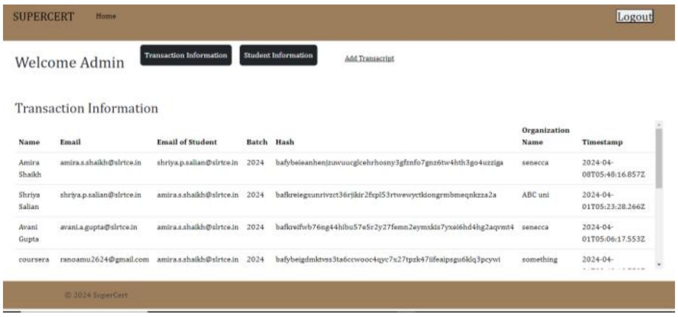

payme.sol - project - Visual Studio Code
studentInfoController.js
deploy.js
payme.json ...\contractJson
payme.sol
cts > payme.sol

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
import {AggregatorV3Interface} from "@chainlink/contracts/src/v0.8/shared/interfa

contract payme {

    address payable owner; //owner is going to receive funds
    constructor(){
        owner = payable(msg.sender);
    }

    uint public amountUsd;

    function fund(int amount) public payable {
        amountUsd = uint(amount);
        owner.transfer(msg.value);
        require(getConversion(msg.value) >= amountUsd, "didnt send enough");
    }

    function getPrice() public view returns (uint256){
        AggregatorV3Interface priceFeed = AggregatorV3Interface(0x694AA1769357215
        (,int256 price ,,,) = priceFeed.latestRoundData();
        return uint(price * 1e10) ;
    }

    function getConversion(uint ethAmount) public view returns (uint256) {
        uint ethPrice = getPrice();
        uint ethAmountInUSD = (ethPrice * ethAmount) / 1e18;
        return ethAmountInUSD;
    }
}
```

Fig. 5. Smart Contract For Payment

Backend Development:

Developing a backend server that communicates with IPFS and the Ethereum blockchain. Which manage file uploads and retrievals, respond to user requests, and communicate with smart contracts. Implement user administration features like verification details and transaction information.



Welcome Admin

Transaction Information

Name	Email	Email of Student	Batch	Hash	Organization Name	Timestamp
Amira Shaikh	amira.s.shaikh@slrtce.in	shriya.p.salian@slrtce.in	2024	bafybeieanhenjzuvuucglcehrhosny3gfznfo7gnz6tw4hth3go4uzziga	senecca	2024-04-08T05:48:16.857Z
Shriya Salian	shriya.p.salian@slrtce.in	amira.s.shaikh@slrtce.in	2024	bafkreiegzunrivzct36rjikir2fxpl53rtwewyctkiongrmbmeqnkzza2a	ABC uni	2024-04-01T05:23:28.266Z
Avani Gupta	avani.a.gupta@slrtce.in	amira.s.shaikh@slrtce.in	2024	bafkreifwb76ng44hibu57e5r2y27femn2eymxkis7yxei6hd4hg2aqvmt4	senecca	2024-04-01T05:06:17.553Z
coursera	ranoamu2624@gmail.com	amira.s.shaikh@slrtce.in	2024	bafybeigdmktvss3ta6ccwooc4qyc7x27tpzk47iifeaipsgu6klq3pcywi	something	2024-04-

Fig. 6. Admin dashboard.

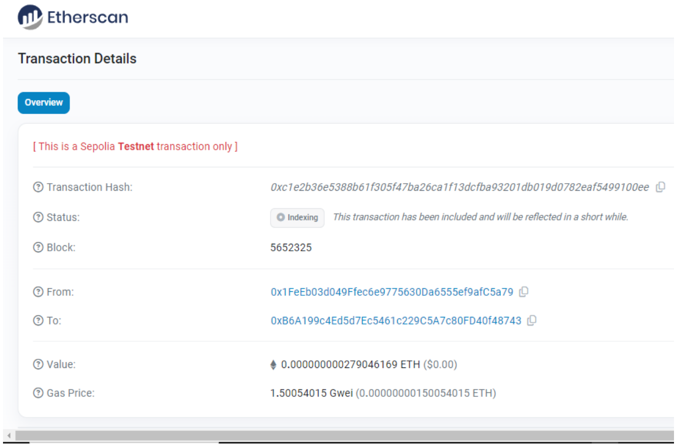
IPFS Integration:

Interacting with IPFS for file storage through Pinata's API. Keeping file contents on IPFS, and for reference, log the resulting IPFS CID hashes in smart contracts and store them in blockchain.

Testing:

Testing the system is secure and operating as intended by thoroughly testing it. Conducting smart contract unit tests. Checking the frontend's compatibility with

Metamask and ease of use. Test Pinata and IPFS file uploads and downloads.


Etherscan

Transaction Details

[This is a Sepolia **Testnet** transaction only]

Transaction Hash: 0xc1e2b36e5388b61f305f47ba26ca1f13dcfba93201db019d0782eaf5499100ee

Status: Indexing This transaction has been included and will be reflected in a short while.

Block: 5652325

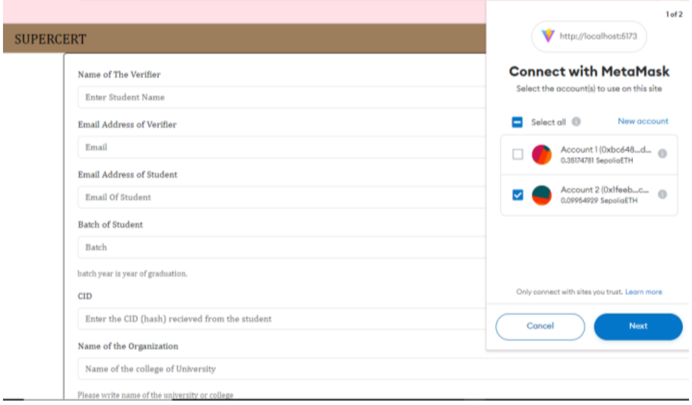
From: 0x1FeEb03d049Ffec6e9775630Da6555ef9afC5a79

To: 0xB6A199c4Ed5d7Ec5461c229C5A7c80FD40f48743

Value: 0.000000000279046169 ETH ($0.00)

Gas Price: 1.50054015 Gwei (0.00000000150054015 ETH)

Fig. 7. Transaction details using Sepolia


SUPERCERT

Name of The Verifier

Enter Student Name

Email Address of Verifier

Email

Email Address of Student

Email Of Student

Batch of Student

Batch

batch year is year of graduation.

CID

Enter the CID (hash) recieved from the student

Name of the Organization

Name of the college of University

Please write name of the university or college

1 of 2

http://localhost:5173

Connect with MetaMask

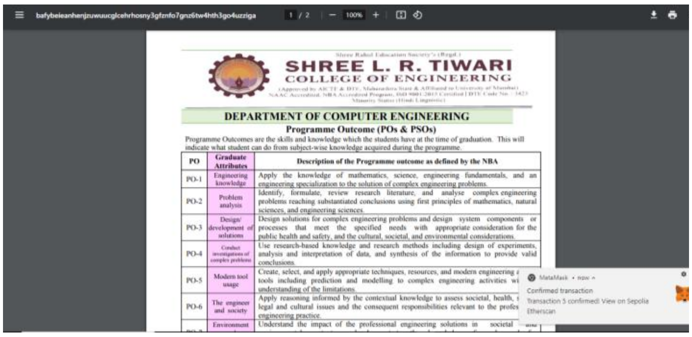
Select the account(s) to use on this site

□ Account 1 (0xbc648...d... 0.35174781 SepoliaETH

☑ Account 2 (0x1feeb...c... 0.09954929 SepoliaETH

Only connect with sites you trust. Learn more

Fig. 8. Testing payment with Metamask.


bafybeieanhenjzuwuucglcehrhosny3gfznfo7gnz6tw4hth3go4uzziga 1 / 2 100%

Shree Rahul Education Society's (Regd.)

SHREE L. R. TIWARI
COLLEGE OF ENGINEERING

(Approved by AICTE & DTE, Maharashtra State & Affiliated to University of Mumbai)
NAAC Accredited, NBA Accredited Program, ISO 9001:2015 Certified | DTE Code No.: 3423
Minority Status (Hindi Linguistic)

DEPARTMENT OF COMPUTER ENGINEERING

Programme Outcome (POs & PSOs)

Programme Outcomes are the skills and knowledge which the students have at the time of graduation. This will indicate what student can do from subject-wise knowledge acquired during the programme.

PO	Graduate Attributes	Description of the Programme outcome as defined by the NBA
PO-1	Engineering knowledge	Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
PO-2	Problem analysis	Identify, formulate, review research literature, and analyse complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO-3	Design/ development of solutions	Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
PO-4	Conduct investigations of complex problems	Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
PO-5	Modern tool usage	Create, select, and apply appropriate techniques, resources, and modern engineering a tools including prediction and modelling to complex engineering activities wi understanding of the limitations.
PO-6	The engineer and society	Apply reasoning informed by the contextual knowledge to assess societal, health, s legal and cultural issues and the consequent responsibilities relevant to the profes engineering practice.
PO-7	Environment	Understand the impact of the professional engineering solutions in societal and

MetaMask • now

Confirmed transaction

Transaction 5 confirmed! View on Sepolia Etherscan

Fig. 9. Testing the after-payment output.

Updating and maintenance:

Monitoring and maintaining your system continuously. implementing improvements and modifications in response to customer feedback and evolving technologies.

The cost of utilizing the system was assessed, including blockchain transaction fees, storage prices, and other costs. The results showed that the pricing was reasonable and competitive, making it an acceptable value for users according to the service provided.

VIII. CONCLUSION

In conclusion, SuperCert represents an advanced and innovative solution for addressing the challenges associated with educational certificates, such as fraud, verification, and data security. Certificates recorded on the blockchain become tamper-proof and can be easily verified by educational institutions and employers. The system incorporates robust identity verification processes to validate the identity of applicants, making it difficult for fraudulent individuals to exploit the system. Data security is a top priority, and SuperCert employs encryption and secure storage mechanisms to protect sensitive user information and certificates. The use of blockchain technology enhances transparency in the certification process, fostering trust among educational institutions. By automating the certificate verification process and reducing the administrative burden on educational institutions, SuperCert improves efficiency in the educational certification ecosystem.

IX. FUTURE SCOPE

The future scopes include working with universities and educational institutions to establish blockchain-based credential verification systems on a larger scale. This might include standardizing the process across numerous colleges and leveraging blockchain technology into current student databases. In addition to educational credentials, blockchain technology can be used to verify professional qualifications, licenses, and legal documents. Exploring the expansion of blockchain verification to these domains could boost trust and transparency across sectors. Constantly upgrading security procedures inside blockchain systems would be required to protect against cyber threats and preserve the integrity of stored certificates. This may include investigating advanced encryption techniques, multi-factor authentication, and biometric verification methods. Promoting widespread use of blockchain-based certificate verification systems on a worldwide scale. This could include raising awareness, offering training and support, and addressing regulatory issues to make implementation easier across multiple countries and jurisdictions. Interoperability, refers to the development of standards and protocols that enable different blockchain networks and systems to communicate with each other. This will enable the easy interchange and verification of certificates across several systems, increasing efficiency and usefulness.

X. REFERENCES

[1] Bessa, Emanuel E., and Joberto SB Martins. "A blockchain-based educational record repository." arXiv preprint arXiv:1904.00315 (2019).

[2] Pathak, Shivani, et al. "Blockchain-based academic certificate verification system—a review." Advanced Computing and Intelligent Technologies: Proceedings of ICACIT 2022 (2022): 527-539.

[3] Bele, Roshani S., and Jayant P. Mehare. "A review on digital degree certificate using blockchain technology." IJCRT 9.2 (2021): 2320-2882.

[4] Saleh, Omar S., Osman Ghazali, and Muhammad Ehsan Rana. "Blockchain based framework for educational certificates verification." Journal of critical reviews (2020).

[5] Chaniago, Nero, Parman Sukarno, and Aulia Arif Wardana. "Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain." Register 7.2 (2021): 149-163.

[6] Raghavender, K. V., et al. "Decentralized Smart Contract Certificate System Using Ethereum Blockchain Technology." Second International Conference on Emerging Trends in Engineering (ICETE 2023). Atlantis Press, 2023.

[7] Doan, Trinh Viet, et al. "Toward decentralized cloud storage with IPFS: opportunities, challenges, and future considerations." IEEE Internet Computing 26.6 (2022): 7-15.

[8] Trautwein, Dennis, et al. "Design and evaluation of IPFS: a storage layer for the decentralized web." Proceedings of the ACM SIGCOMM 2022 Conference. 2022.

[9] Alizadeh, Morteza, Karl Andersson, and Olov Schelén. "Efficient decentralized data storage based on public blockchain and IPFS." 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). IEEE, 2020.

[10] Singh, Akanksha, Harsh Vardhan Gupta, and Vaishnavi Gupta. "Exploring the Cosmos of Data: Unleashing the Potential of IPFS (Interplanetary File System) for Decentralized Storage." Vidhyayana-An International Multidisciplinary Peer-Reviewed E-Journal-ISSN 2454-8596 8.6 (2023).

[11] Hujare, Ankush R., et al. "DECENTRALIZED FILE SYSTEM USING BLOCKCHAIN."

[12] Enwerem, Udochukwu C. "BLOCKCHAIN RESULT AND TRANSCRIPT MANAGEMENT SYSTEM: A CASE STUDY OF FEDERAL UNIVERSITY OF TECHNOLOGY OWERRI." International Conference on Communication and E-Systems For Economic Stability| CeSES. 2023.

[13] Mohanty, Debasis, et al. "Blockchain interoperability: Towards a sustainable payment system." Sustainability 14.2 (2022): 913.

[14] Kuonen, David. "The process of creating, testing, and deploying smart contracts on the Ethereum blockchain using Solidity." (2023).

[15] Soares, Pamella, et al. "Extending the Docstone to Enable a Blockchain-based Service for Customizable Assets and Blockchain Types."

Journal of Software Engineering Research and Development 11.1 (2023): 15-1.

[16] Das, Moumita, et al. "A blockchain-based integrated document management framework for construction applications." Automation in Construction 133 (2022): 104001.

[17] Imam, Iftekher Toufique, et al. "DOC-BLOCK: A blockchain based authentication system for digital documents." 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). IEEE, 2021.

[18] ONWUASOANYA, NC, and BE EZE. "MYTRANSCRIPT: AN ACADEMIC TRANSCRIPT DECENTRALISED WEB APPLICATION SYSTEM BASED ON THE ETHEREUM BLOCKCHAIN." (2022).

[19] Shakan, Yassynzhan, et al. "Verification of university student and graduate data using blockchain technology." International Journal of Computers Communications & Control 16.5 (2021).

[20] Meirobie, Isyak, et al. "Framework Authentication e-document using Blockchain Technology on the Government system." International Journal of Artificial Intelligence Research 6.2 (2022).