



TAGORE ENGINEERING COLLEGE



SB8055 – BLOCK CHAIN DEVELOPMENT

DATE	30 OCTOBER 2023
TEAM ID	NM2023TMID01010
PROJECT NAME	Transparent Education Management System

TEAM LEADER	SAKTHIGOMATHI.S
TEAM MEMBER 1	ROSELIN GRACY.I
TEAM MEMBER 2	MOHANA PRIYA.M
TEAM MEMBER 3	SANDHIYA.N



1. **INTRODUCTION**
 - 1.1 Project Overview
 - 1.2 Purpose
2. **LITERATURE SURVEY**
 - 2.1 Existing problem
 - 2.2 References
 - 2.3 Problem Statement Definition
3. **IDEATION & PROPOSED SOLUTION**
 - 3.1 Empathy Map Canvas
 - 3.2 Ideation & Brainstorming
4. **REQUIREMENT ANALYSIS**
 - 4.1 Functional requirement
 - 4.2 Non-Functional requirements
5. **PROJECT DESIGN**
 - 5.1 Data Flow Diagrams & User Stories
 - 5.2 Solution Architecture
6. **PROJECT PLANNING & SCHEDULING**
 - 6.1 Technical Architecture
 - 6.2 Sprint Planning & Estimation
 - 6.3 Sprint Delivery Schedule
7. **CODING & SOLUTIONING (Explain the features added in the project along with code)**
 - 7.1 Feature 1
 - 7.2 Feature 2
 - 7.3 Database Schema
8. **PERFORMANCE TESTING**
 - 8.1 Performance Metrics
9. **RESULTS**
 - 9.1 Output Screenshots
10. **ADVANTAGES & DISADVANTAGES**
11. **CONCLUSION**
12. **FUTURE SCOPE**
13. **APPENDIX**
 - Source Code
 - GitHub & Project Demo Link

1. INTRODUCTION

1.1 Project Overview:

The Decentralized Student Certificate Management System is a cutting-edge solution designed to enhance transparency, security, and accessibility in the management of student certificates. Leveraging blockchain technology and smart contracts, this project aims to provide a decentralized platform for issuing, storing, and verifying digital certificates.

Key Features:

Blockchain Integration: Utilizes Ethereum blockchain for transparent and immutable ledger of certificate data.

Smart Contracts: Implements smart contracts to define certificate structure, issuance logic, and verification processes.

Decentralized Storage: Utilizes IPFS for secure storage and distribution of digital certificate files.

Certificate Issuance: Enables issuing authorities to create digital certificates, recording details on the blockchain.

Certificate Verification: Provides a user-friendly interface for querying and verifying certificate details using unique certificate IDs.

Security Measures: Implements robust encryption and public-private key cryptography for data security and validation.

User Interface: Optional web or mobile interface for easy access, ensuring a seamless user experience.

Regular Auditing: Regularly audits the system for security vulnerabilities, ensuring a reliable and trustworthy platform.

Benefits:

Transparency: Transparent and publicly accessible ledger ensures integrity and authenticity of certificates.

Security: Strong encryption and decentralized storage enhance security, preventing unauthorized access or tampering.

Efficiency: Streamlines the certificate verification process, reducing time and effort for both institutions and certificate holders.

Accountability: Immutability of blockchain records ensures accountability in the management of student credentials.

Target Audience:

Educational institutions, employers, and students seeking a reliable and secure method for managing and verifying digital certificates.

Outcome: The Decentralized Digital Certificate Management System revolutionizes the way educational credentials are managed and verified, fostering trust and efficiency in the education sector and beyond.

1.2 Purpose:

The purpose of the Decentralized Digital Certificate Management System is to revolutionize the traditional education credentialing process. By harnessing the power of blockchain technology, the system aims to establish a secure, transparent, and efficient platform for issuing, storing, and verifying digital certificates. This innovative solution enhances trust, eliminates fraud, and simplifies the verification process for educational institutions, employers, and students, ensuring the integrity and credibility of academic achievements in a digital age.

2. LITERATURE SURVEY

Authors	Published year	Topics	Type of source	Summary
Johnson, M. Smith, A.,Lee, K.	2018	"Blockchain Technology in Education: The Future of Learning"	Article	This paper explores the potential of blockchain technology in revolutionizing the education sector. It discusses the advantages of using blockchain for creating and verifying digital certificates, ensuring data security and transparency.
Chen, L.Wang, S. Zhang, J.	2017	"Enhancing Transcript Security using Blockchain Technology"	Book	This research paper focuses on the application of blockchain to enhance the security of academic transcripts. It delves into the cryptographic techniques and decentralized nature of blockchain, ensuring the authenticity of digital certificates and transcripts. 3. "Blockchain-based Academic Credential Verification"
Kumar, A.Yadav, D.Singh, R.	2019	"Blockchain-based Academic Credential Verification"	Book	The paper discusses the implementation of blockchain technology for academic credential verification. It explores the challenges faced by traditional certificate verification systems and how blockchain can address these issues, providing a tamper-proof and reliable solution.
White, J.Leifer, L. J.	2016	"Blockchain in Education: Surveying the Landscape"	Article	This survey provides an overview of blockchain applications in education. It covers digital certificates, academic record keeping, and discusses the potential challenges and future prospects of integrating blockchain technology in educational institutions.
Hobohm, S. Budroni, A. Marenzi, I.	2019	"Blockchain in Education: A Review and a Research Agenda"	Book	The authors present a comprehensive review of blockchain applications in the education sector. The survey points out the benefits of using blockchain for digital certificates, emphasizing the need for standardization and interoperability across educational institutions. These literature pieces and survey points highlight the advancements and challenges in implementing blockchain technology for creating digital

				certificates. They emphasize the importance of data security, transparency, and the potential transformative impact on the education sector
--	--	--	--	---

Problem statement Definition

Problem Statement:

In today's digital age, the issuance and verification of academic certificates face challenges related to security, authenticity, and accessibility. Traditional methods of storing certificates are susceptible to fraud and loss. Moreover, the centralized nature of certificate storage systems can lead to single points of failure and privacy concerns. There is a need for a secure, decentralized, and tamper-proof system to store digital certificates while ensuring easy verification and accessibility for relevant stakeholders.

Problem Definition:

The challenge is to design a decentralized and distributed solution for storing digital certificates securely and efficiently. The system must leverage blockchain technology to create an immutable ledger of academic achievements. This ledger should be distributed across multiple nodes, ensuring that no single entity has control over the entire network. The solution must allow for the addition of new certificates and enable easy querying of certificate details from the blockchain

3. IDEATION & PROPOSED SOLUTION


3.1 EMBATHY MAP CANVAS



3.2 IDEATION & BRAINSTORMING

STEP 1 Define your Problem Statement:

Temp!



Brainstorm & idea prioritization

Use this template in your own brainstorming sessions so your team can unleash their imagination and start shaping concepts even if you're not sitting in the same room.

⌚ 10 minutes to prepare
🕒 1 hour to collaborate
👤 2-8 people recommended

➔

Before you collaborate

A little bit of preparation goes a long way with this session. Here's what you need to do to get going.

⌚ 10 minutes

1

Define your problem statement

What problem are you trying to solve? Frame your problem as a How Might We statement. This will be the focus of your brainstorm.

⌚ 5 minutes

4

Team gathering

Define who should participate in the session and send an invite. Share relevant information or pre-work ahead.

5

Set the goal

Think about the problem you'll be focusing on solving in the brainstorming session.

6


Learn how to use the facilitation tools

Use the Facilitation Superpowers to run a happy and productive session.

[Open article](#) ➔


PROBLEM


Blockchain is a technology designed to manage education data that has the potential to support transparency and accountability. A blockchain is a ledger of transactions where an identical copy is visible to all the members of a computer network. Network members validate the data entered into the ledger, and once entered, the data is immutable. Design a solution where you can store the digital certificates of the students in a distributed and decentralized network. You should be able to add the certificated details into the blockchain query the certificate details from the blockchain.





Key rules of brainstorming


To run an smooth and productive session


 Stay in topic.

 Listen to others. Encourage wild ideas.

 Defer judgment.

 Encourage wild ideas.

 Go for volume.

 If possible, be visual.

STEP 2 Group ideas

2

Brainstorm

Write down any ideas that come to mind that address your problem statement.

⌚ 10 minutes

Sakthi Gomathi.S.

Select a blockchain platform that suits your requirements, such as Ethereum, Hyperledger Fabric, or Binance Smart Chain. Consider factors like scalability, security, and ease of use.

Create smart contracts specifying the structure of digital certificates. Include fields like student name, course, grade, date, and any other necessary details. Ensure that the smart contracts are secure and tamper-proof.

Implement a decentralized identity management system (e.g., Self-Sovereign Identity) to empower students with control over their certificates. This system allows students to manage their identities and certificates without relying on a central authority.

Mohanapriya.M

Store the actual digital certificates off-chain (outside the blockchain) due to space and cost considerations. Use decentralized storage solutions like IPFS (InterPlanetary File System) to store the certificates securely. Store the IPFS hash or the link to the certificate on the blockchain.

When a student completes a course, an authorized issuer (such as a school or university) creates a digital certificate. The certificate details are then hashed and stored on the blockchain, linking to the actual certificate on IPFS.

Network participants validate the data entered into the ledger. Once validated, the certificate data becomes immutable, ensuring its integrity. Use consensus algorithms to verify the authenticity of transactions.

Roselin Gracy.I

Implement a user identity interface (such as a web application or mobile app) that allows authorized parties (e.g., employers, educational institutions) to query certificate details from the blockchain. Users can search for certificates using unique identifiers like student ID or certificate number.

Implement access control mechanisms to protect sensitive information. Define rules and permissions to ensure that only authorized users can view or update specific certificate details.

Periodically audit the system to ensure its security and integrity. Update smart contracts and system components as needed to adapt to changing requirements or emerging technologies.

Sandhiya.N

Provide documentation and educational resources to users, explaining how to interact with the decentralized certificate system. This step is crucial for widespread adoption and understanding.

Implementing a blockchain solution requires a good understanding of blockchain technology, smart contracts, and decentralized systems. It's advisable to collaborate with experienced blockchain developers and security experts to ensure the system's robustness and reliability.

Network participants validate the data entered into the ledger. Once validated, the certificate data becomes immutable, ensuring its integrity. Use consensus algorithms to verify the authenticity of transactions.

Group ideas

Take turns sharing your ideas while clustering similar or related notes as you go. Once all sticky notes have been grouped, give each cluster a sentence-like label. If a cluster is bigger than six sticky notes, try and see if you can break it up into smaller sub-groups.

🕒 20 minutes

TIP

Add customizable tags to sticky notes to make it easier to find, browse, organize, and categorize important ideas as themes within your mural.

Implement a decentralized identity management system (e.g., Self-Sovereign Identity) to empower students with control over their certificates. This system allows students to manage their identities and certificates without relying on a central authority.

Network participants validate the data entered into the ledger. Once validated, the certificate data becomes immutable, ensuring its integrity. Use consensus algorithms to verify the authenticity of transactions.

Periodically audit the system to ensure its security and integrity. Update smart contracts and system components as needed to adapt to changing requirements or emerging technologies.

Network participants validate the data entered into the ledger. Once validated, the certificate data becomes immutable, ensuring its integrity. Use consensus algorithms to verify the authenticity of transactions.

STEP 4 Prioritize

4

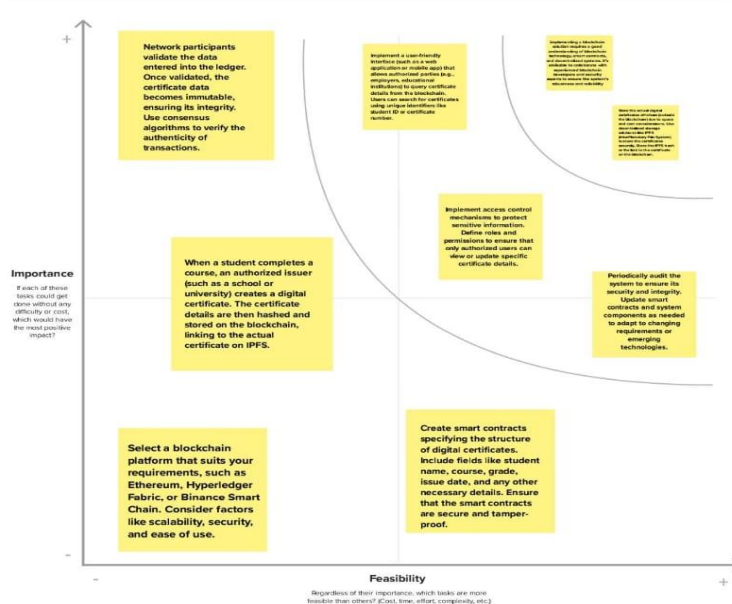
Prioritize

Your team should all be on the same page about what's important moving forward. Place your ideas on this grid to determine which ideas are important and which are feasible.

🕒 20 minutes

TIP

Participants can use their cursors to point at where sticky notes should go on the grid. The facilitator can confirm the spot by using the laser pointer holding the H key on the keyboard.



+

After you collaborate

You can export the mural as an image or pdf to share with members of your company who might find it helpful.

Quick add-ons

- Share the mural**
Share a view link to the mural with stakeholders to keep them in the loop about the outcomes of the session.
- Export the mural**
Export a copy of the mural as a PNG or PDF to attach to emails, include in slides, or save in your drive.

Keep moving forward

- Strategy blueprint**
Define the components of a new idea or strategy.
[Open the template →](#)
- Customer experience journey map**
Understand customer needs, motivations, and obstacles for an experience.
[Open the template →](#)
- Strengths, weaknesses, opportunities & threats**
Identify strengths, weaknesses, opportunities, and threats (SWOT) to develop a plan.
[Open the template →](#)

[Share template feedback](#)

4 REQUIREMENT ANALYSIS

4.1 FUNCTIONAL REQUIREMENTS

Certificate Issuance:

The system must allow issuing authorities to create digital certificates.

Certificates should include student name, course, completion date, and a unique identifier.

Blockchain Integration:

The system must integrate with a suitable blockchain platform (e.g., Ethereum) to store certificate data immutably.

Smart Contract Development:

Smart contracts must be developed to manage certificate creation, storage, and verification processes.

Decentralized Storage:

The system should use IPFS or a similar solution for decentralized and secure storage of digital certificate files.

Certificate Verification:

Users should be able to query certificate details using a unique certificate ID.

The system must provide real-time verification of certificate authenticity.

Security Measures:

Strong encryption techniques must be employed to secure certificate data and transactions.

Public-private key pairs should be used for secure authentication and validation.

User Interface:

Optional user interface (web or mobile app) for users to input certificate ID and view certificate details.

4.2 NON-FUNCTIONAL REQUIREMENTS

Performance:

The system must handle a large number of transactions efficiently.

Response time for certificate verification requests should be minimal.

Security:

The system should be resistant to unauthorized access, ensuring data privacy.

Regular security audits and updates are necessary to address vulnerabilities.

Scalability:

The solution should be scalable to accommodate an increasing number of certificates and users over time.

Reliability:

The system must be available and reliable 24/7 to facilitate certificate verification whenever needed.

Compliance:

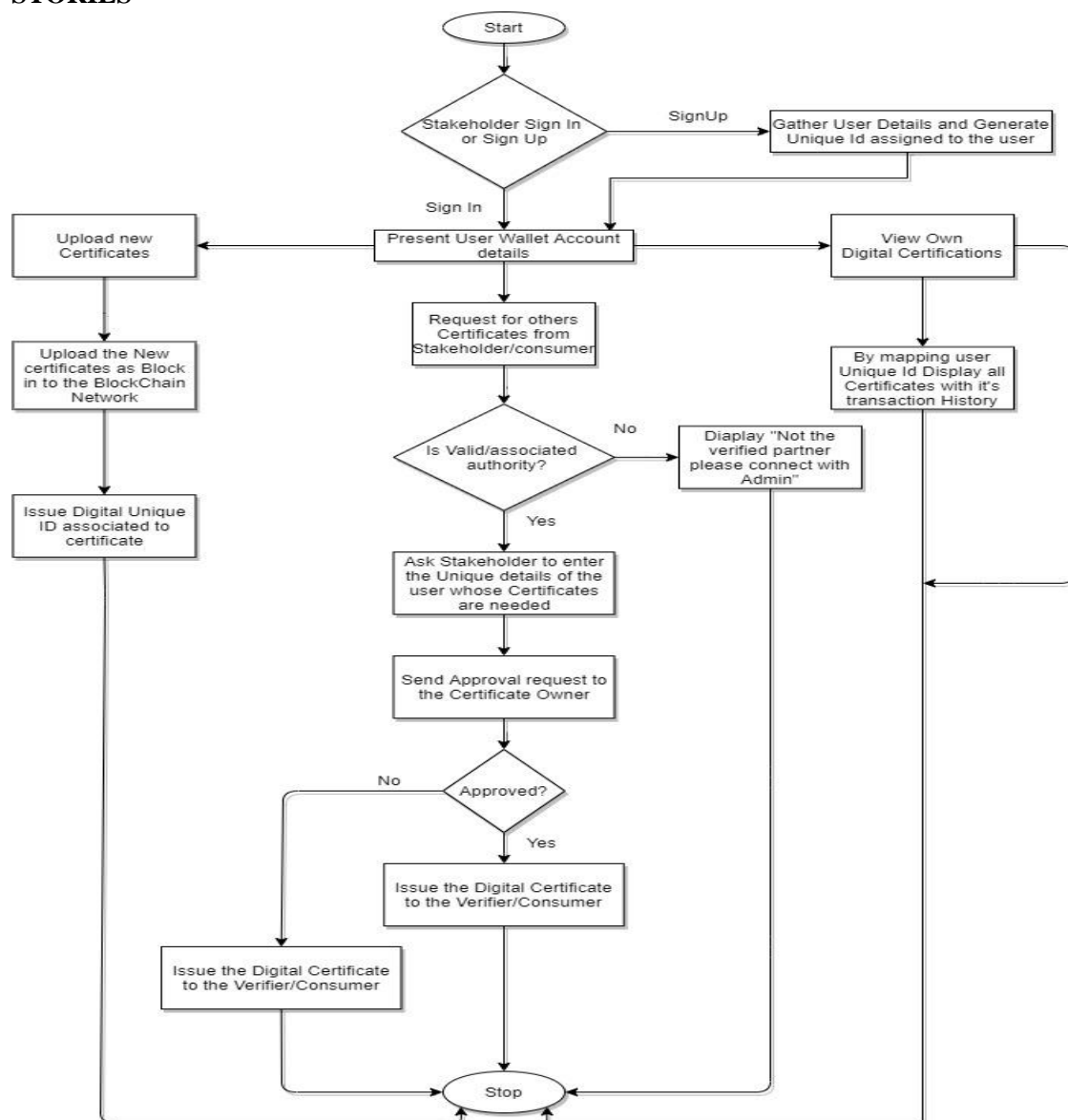
The solution must comply with data protection regulations and industry standards for digital credentialing.

Interoperability:

The system should be designed to integrate with existing educational databases and verification systems.

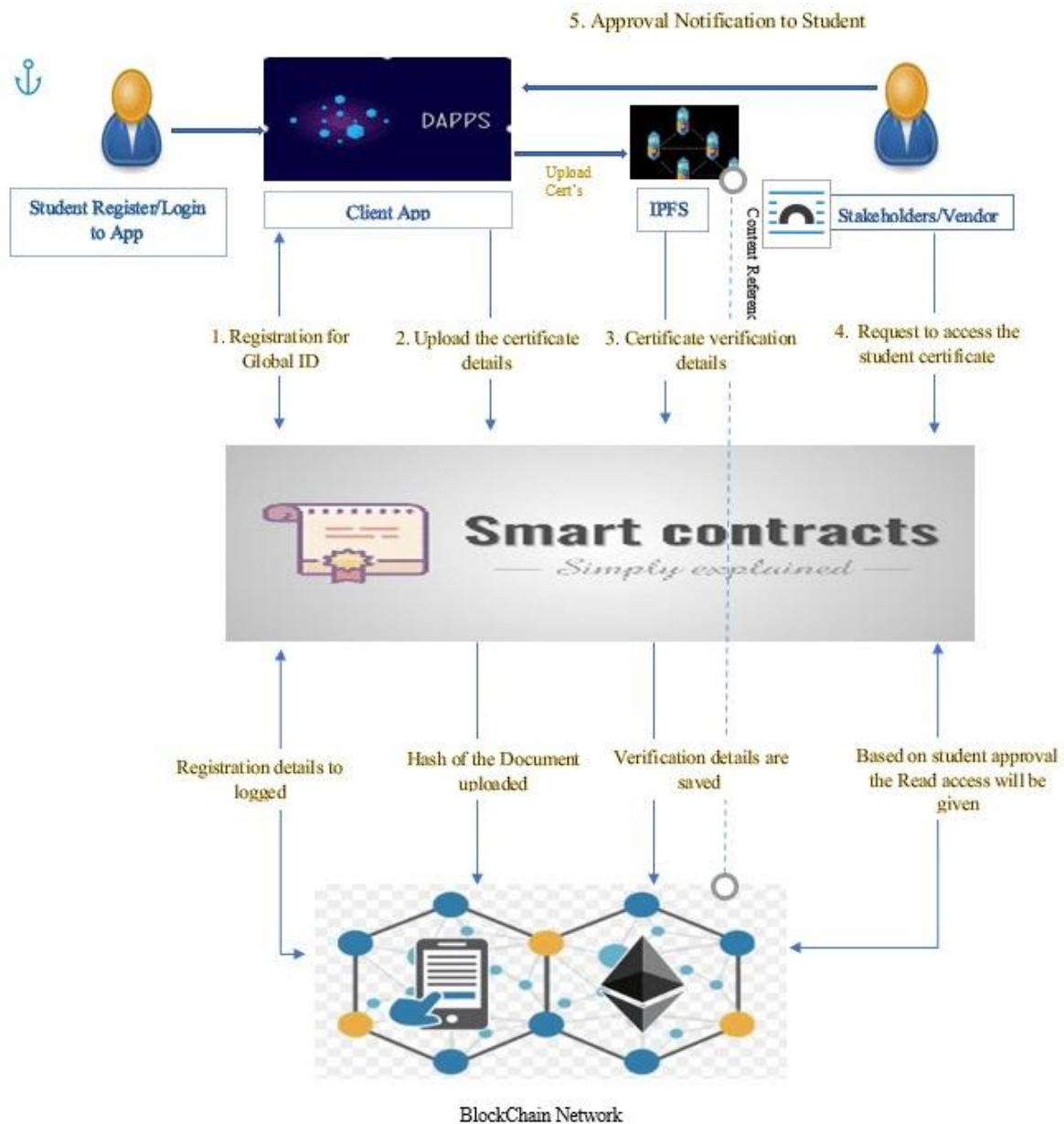
5. PROJECT DESIGN

5.1 DATA FLOW DIAGRAMS AND USER STORIES



The data flow diagram for the digital certificates of student

5.2 Solution Architecture



6. PROJECT PLANNING AND SCHEDULING

6.1 Technical Architecture

Blockchain Platform Selection:

Fabric, or Choose a suitable blockchain platform like Ethereum, Hyperledger any other that supports smart contracts and decentralized applications.

Smart Contract Development:

Develop a smart contract for managing digital certificates. The smart contract should include functions for adding certificate details and querying certificate information.

Decentralized Storage:

Utilize decentralized storage systems like IPFS (Inter Planetary File System) to store the actual digital certificate files. Store the IPFS hash or other decentralized storage references in the blockchain. This ensures that certificate files are distributed across the network.

Certificate Metadata:

Store certificate metadata such as student name, ID, course details, and issuance date in the blockchain. Use a structured format like JSON to store this information.

Identity Management:

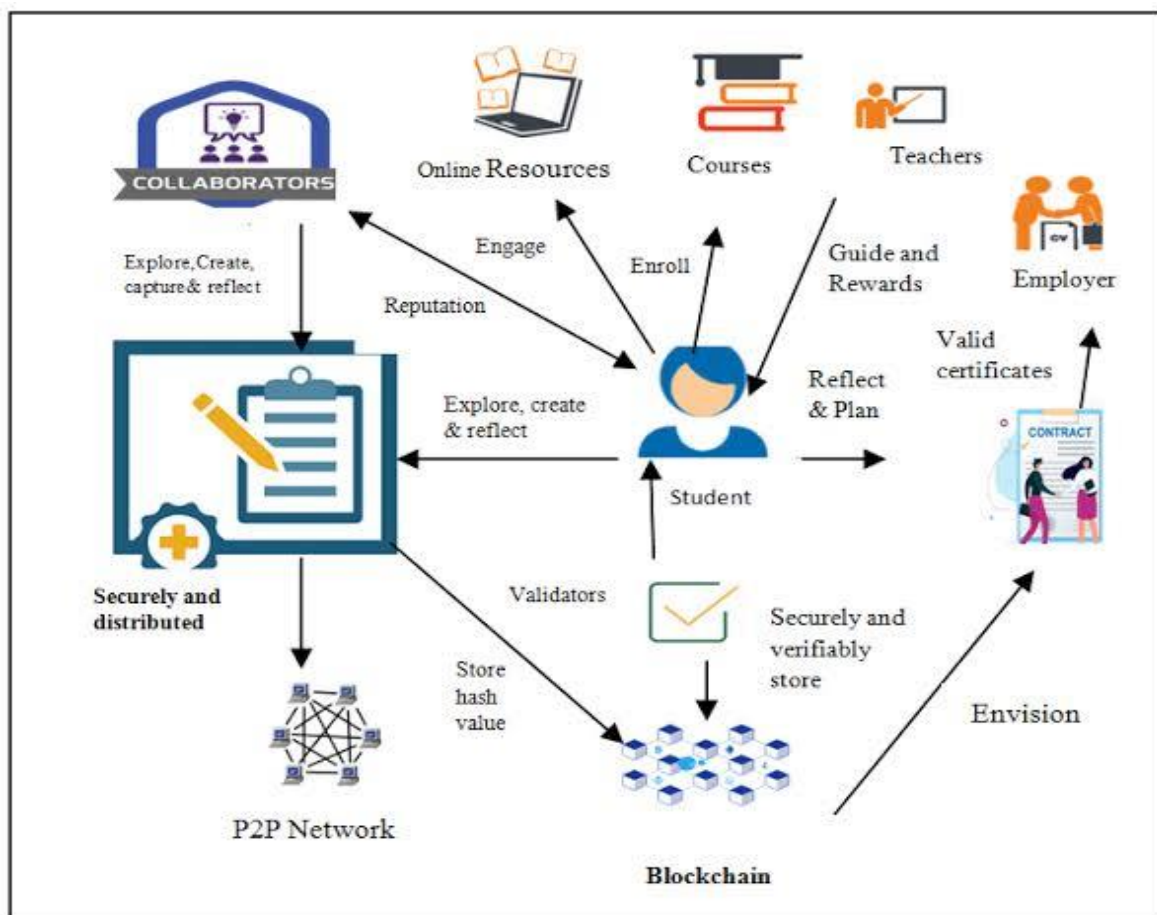
Implement a secure identity management system. You can use cryptographic techniques to verify the identity of the entities involved in adding or querying certificate details.

User Interface:

Develop a user interface for students, educational institutions, and employers to interact with the blockchain. This interface should allow students to request certificates, educational institutions to issue certificates, and employers to verify certificates.

Transaction Validation:

Implement consensus mechanisms and validation rules within the smart contract to ensure that only valid and authorized transactions are added to the blockchain. This enhances security and prevents tampering.



Solution architecture

6.2 SPRINT PLANNING:

TITLE	DESCRIPTION	DATE
Specify the business problem	Inefficient and centralized Education management systems hinder accessibility, transparency, and security, leading to suboptimal user experiences.	October 9 2023
Literature survey and information gathering	Explore existing literature on blockchain applications in Education management, identifying successes, challenges, and best practices.	October 10 2023
Prepare empathy map	Understand the needs and pain points of students, staffs and administrators to inform the design process.	October 11 2023
Ideation	Brainstorm innovative features and functionalities, such as decentralized cataloging, transparent transaction history, and user-friendly interfaces.	October 15 2023
Solution architecture	Design a robust blockchain based architecture, outlining the integration of smart contracts, decentralized storage, and a user-friendly front end.	October 18 2023

Business requirements	Define the functional and nonfunctional requirements, ensuring alignment with stakeholders' expectations and industry standards.	October 19 2023
Data flow diagram	Illustrate the flow of information within the system, emphasizing how blockchain ensures data integrity and traceability	October 19 2023
Technology architecture	Specify the technologies required, including blockchain platforms, programming languages, and database systems	October 19 2023
Project development	Break down the development process into sprints, focusing on iterative implementation, testing, and user feedback to ensure a successful and user friendly library management solution	October 20 2023

6.3 Sprint Delivery and Schedule

Sprint 1: Planning and Blockchain Setup

Week 1-2:

Define detailed requirements and specifications for the smart contract.

Choose a suitable blockchain platform and set up the development environment.

Sprint 2: Smart Contract Development

Week 3-4:

Develop the smart contract for adding and querying certificate details.

Implement basic error handling and security features in the contract.

Sprint 3: Decentralized Storage Integration

Week 5-6:

Integrate IPFS for storing certificate files.

Modify the smart contract to store IPFS hashes of certificates.

Sprint 4: DApp Development - Part 1

Week 7-8:

Design the user interface for uploading certificate details.

Implement basic user authentication using blockchain-based identity solutions.

Sprint 5: DApp Development - Part 2

Week 9-10:

Connect the DApp interface with the smart contract functions.

Add functionality for users to query certificates based on student IDs.

Sprint 6: Testing and Security Enhancement

Week 11-12:

Conduct extensive testing of the entire system, including smart contract functions and DApp interfaces.

Implement additional security measures such as encryption for stored certificates.

Sprint 7: Documentation and Deployment

Week 13-14:

Document the entire system, including smart contract details, DApp usage guide, and security protocols. Deploy the solution on a testnet for final testing by stakeholders. Prepare for the production deployment.

7. CODING AND SOLUTIONING:

```
// SPDX-License-Identifier: MIT
```

```
pragma solidity ^0.8.0;
```

```
contract collegeCertificate {  
    address public owner;
```

```
    struct Certificate {  
        string studentName;  
        string courseName;  
        uint256 DateOfGraduation;
```

```

    uint256 issueDate;

    address issuer;
}

uint256 public totalCertificates;
mapping(uint256 => Certificate) public certificates;

event CertificateIssued(
    uint256 indexed certificateId,
    string studentName,
    string courseName,
    uint256 issueDate,
    address indexed issuer
);

constructor() {
    owner = msg.sender;
}

modifier onlyOwner() {
    require(msg.sender == owner, "Only contract owner can call this");
    _;
}

function issueCertificate(
    string memory studentName,
    string memory courseName,
    uint256 _dateOfGraduation,
    uint256 issueDate
) external onlyOwner {
    uint256 certificateId = totalCertificates + 1;

```



```

certificates[certificateId] = Certificate({
    studentName: studentName,
    courseName: courseName,
    DateOfGraduation : _dateOfGraduation,
    issueDate: issueDate,
    issuer: msg.sender
});

totalCertificates = certificateId;

emit CertificateIssued(
    certificateId,
    studentName,
    courseName,
    issueDate,
    msg.sender
);
}

function getCertificate(
    uint256 certificateId
) external view returns (string memory, string memory, uint256, uint256, address) {
    Certificate memory cert = certificates[certificateId];
    return (cert.studentName, cert.courseName, cert.DateOfGraduation, cert.issueDate,
cert.issuer);
}
}

```

8. PERFORMANCE TESTING

8.1 Performance metrics

TITLE	DESCRIPTION
Transaction Throughput	Measure the number of certificate addition transactions processed per second to assess the system's processing capacity.
Transaction Confirmation Time	Evaluate the average time taken to confirm a certificate addition transaction on the blockchain. Lower confirmation time indicates faster transaction processing
Query Response Time	Measure the time taken to retrieve certificate details based on student IDs.
Storage Efficiency	Calculate the ratio of blockchain storage space used for certificates' metadata (e.g., IPFS hashes) to the actual size of certificates stored. Optimize for efficient use of storage resources.
Security Metrics	Assess the encryption strength, data integrity, and resistance to tampering to ensure the security of stored certificate information.
Network Latency	Evaluate the delay in communication between nodes in the distributed network to optimize data transmission speed.
Resource Utilization	Monitor CPU, memory, and bandwidth usage to ensure the system operates within acceptable resource limits, optimizing for performance.

9. RESULTS

Issue Certificate On Blockchain

Connect Wallet

Issuance of Certificate on Blockchain

get Certificate

10. ADVANTAGES & DISADVANTAGES

ADVANTAGES

1. Transparency and Trust:

Certificates are publicly verifiable, ensuring transparency and trust in the education system.

2. Security:

Blockchain's cryptographic techniques provide a high level of security, making it difficult to tamper with or counterfeit certificates.

3. Decentralization:

Decentralized nature eliminates the need for a central authority, reducing the risk of single points of failure and ensuring data integrity.

4. Accessibility:

Certificates can be accessed and verified from anywhere, providing convenient access to both students and employers.

5. Immutable Records:

Once added to the blockchain, certificate records are immutable, ensuring a permanent and unchangeable record of achievements.

DISADVANTAGES:

1. Scalability:

Blockchain networks, especially public ones like Ethereum, might face scalability issues when processing a large volume of transactions, leading to delays.

2. Energy Consumption:

Proof-of-work blockchains, like Bitcoin and Ethereum (currently), consume significant amounts of energy, raising environmental concerns.

3. Privacy Concerns:

Public blockchains are transparent, which might raise privacy concerns as personal information, even though hashed, is visible on the blockchain.

4. Initial Development Complexity:

Developing smart contracts and integrating them with decentralized storage can be complex and time-consuming, requiring skilled developers.

5. Regulatory Challenges:

Legal and regulatory frameworks around blockchain and digital certificates might vary across jurisdictions, posing challenges for implementation.

11. CONCLUSION

Implementing a solution where digital certificates are stored in a distributed and decentralized network using blockchain technology offers unparalleled transparency, security, and accessibility. The blockchain ensures the integrity and immutability of certificate records, making them tamper-proof and easily verifiable by anyone, anywhere.

By utilizing a decentralized storage system like IPFS, the system not only benefits from the security of blockchain but also ensures the availability and redundancy of certificate files across a network of nodes.

However, it's crucial to consider the evolving landscape of blockchain technology, especially concerning scalability, energy efficiency, and regulatory compliance. Despite these challenges, the advantages of a decentralized and transparent certification system significantly outweigh the disadvantages, making it a powerful and promising solution for the future of education and credential verification.

12. FUTURE SCOPE

Enhanced Security Measures:

Implement advanced cryptographic techniques to further enhance the security of digital certificates, ensuring they remain secure against evolving cyber threats.

Integration with IoT Devices:

Explore integration possibilities with IoT devices to automate the issuance process securely. IoT sensors could verify student attendance or completion of practical tasks, triggering the issuance of certificates automatically.

Interoperability with Other Blockchains:

Work on interoperability protocols to enable the exchange of certificate data between different blockchain networks. This would facilitate seamless verification across various educational institutions and industries.

Integration with Learning Management Systems (LMS):

Integrate the blockchain-based certification system with popular Learning Management Systems, making it easier for educational institutions to issue certificates and for students to access and share them securely.

Digital Identity Management:

Explore the integration of digital identity solutions, allowing students to have control over their personal data and certificates. Self-sovereign identity principles can be applied, giving individuals ownership of their digital identities and certificates.

Smart Contract Upgrades:

Continuously enhance smart contracts to include additional features such as certificate revocation mechanisms, allowing institutions to revoke certificates in case of fraud or misconduct.

Global Recognition and Standardization:

Work towards global recognition and standardization of blockchain-based digital certificates. Collaborate with international educational bodies and industry organizations to establish universal standards for digital certificates, ensuring their acceptance worldwide.

Research in Quantum Computing Resistance:

Invest in research to make the system quantum computing-resistant, ensuring the long-term security of digital certificates as quantum computing technology advances.

13 APPENDIX:

github link:

<https://github.com/sakthi334/Transparent-education-Management-System-NM2023TMID01010>

Project Demo Link:

<https://youtu.be/4NbACXqcW2Q?si=IsB6Bj8M3084PEZz>