PROJECT REPORT

ON

DOCUMENT VERIFICATION AND MANAGEMENT SYSTEM USING BLOCKCHAIN

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE DEGREE OF

BACHELOR OF ENGINEERING

In

COMPUTER ENGINEERING

By

Gaytri Kumari	**Roll No.: B400430169**
Pandey Nidhi Mataprasad	**Roll No.: B400430236**
Tiya Mukherjee	**Roll No.: B400430306**

Under the Guidance of

Prof. P. R. Dongre

Sinhgad Institutes

Submitted to

DEPARTMENT OF COMPUTER ENGINEERING

STES'S SINHGAD ACADEMY OF ENGINEERING, PUNE-411048

2024 -2025

Sinhgad Institutes

CERTIFICATE

This is to certify that the Project Report entitled

DOCUMENT VERIFICTAION AND MANAGEMENT SYSTEM USING BLOCKCHAIN

Submitted By

Gaytri Kumari **Roll No.: B400430169**

Pandey Nidhi Mataprasad **Roll No.: B400430236**

Tiya Mukherjee **Roll No.: B400430306**

Is a bonafide work carried out by them under the supervision by **Prof. P.R. Dongre** and it is approved for the partial fulfilment of the requirement of **Savitribai Phule Pune University** for the Project in the Final Year of Computer Engineering.

Prof. P.R. Dongre	***Prof. S.N.Shelke***	***Dr. K. P. Patil***
Guide	***H.O.D***	***Principal***
Dept. of Computer Engg.	***Dept. of Computer Engg.***	***SAOE, Pune***

Place: Pune ***External Examiner*** ***Prof. P.J.Hajare***

Date: / /2025 ***Project Co-ordinator***

ACKNOWLEDGEMENT

We would like to take this opportunity to thank all the people who were part of this seminar in numerous ways, people who gave un-ending support right from the initial stage.

In particular we wish to thank **Prof. P. R. Dongre** as internal project guide who gave their co-operation timely and precious guidance without which this project would not have been a success. We thank them for reviewing the entire project with painstaking efforts and more of his, unbanning ability to spot the mistakes.

We would like to thank our **H.O.D Prof. S. N. Shelke** for his continuous encouragement, support and guidance at each and every stage of project.

And last but not the least we would like to thank all my friends who were Associated with me and helped me in preparing my project. The project named **"DOCUMENT VERIFICTAION AND MANAGEMENT SYSTEM USING BLOCKCHAIN"** would not been possible without the extensive support of people who were directly or indirectly involved in its successful execution.

Project Group Members:

Gaytri Kumari	**Roll No.: B400430169**
Pandey Nidhi Mataprasad	**Roll No.: B400430236**
Tiya Mukherjee	**Roll No.: B400430306**

ABSTRACT

The issuance and verification of professional certificates are fundamental for career progression, yet existing systems are often slow, labour-intensive, and vulnerable to fraud. This project addresses these challenges by leveraging blockchain technology, specifically the Ethereum platform and smart contracts, to enhance the security, efficiency, and transparency of certification processes. By converting traditional paper certificates into digital formats and applying cryptographic hash functions, unique hash values are generated and stored on the blockchain. This approach ensures a clear, immutable record of certifications, streamlining both issuance and verification. Using a unique certificate ID and transaction hash, users and third parties can verify credentials securely and instantly through a unified platform. This system not only simplifies certificate management but also mitigates forgery risks, unauthorized modifications, and administrative overhead, demonstrating a scalable, secure solution for the digital future of credentialing.

Keywords: Blockchain technology, Ethereum platform, professional certificates, smart contracts, cryptographic hash, certificate verification, forgery prevention, digital credentials, credential authentication, immutable record.

Table of Contents

LIST OF ABBREVATIONS

ABBREVIATION	ILLUSTRATION
DMS	Document Management System
UI	User Interface
UX	User Experience
IPFS	InterPlanetary File System
UUID	Universally Unique Identifier
CID	Content Identifier
SDLC	Software Development Life Cycle
API	Application Programming Interface
UX/UI	User Experience/User Interface
HTML	HyperText Markup Language
CSS	Cascading Style Sheets
JS	JavaScript
EVM	Ethereum Virtual Machine
SHA-256	Secure Hash Algorithm 256-bit
DRY	Don’t Repeat Yourself (coding principle)
DAG	Directed Acyclic Graph
DHT	Distributed Hash Table
PKI	Public Key Infrastructure
P2P	Peer-to-Peer
VS Code	Visual Studio Code
ETH	Ethereum (cryptocurrency)

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

INTRODUCTION

1.1 OVERVIEW

The idea of blockchain technology was originally defined by research scientists Stuart Haber and W. Scott Stornetta, but it gained prominence in 2009 when Bitcoin was created by Satoshi Nakamoto. Blockchain technology is today prevalent in the education field for various applications, such as issuing and authenticating documents (e-transcripts), low-cost bulk file storage, automated learning platforms, publishing and copyrighting, and payment through cryptocurrencies. Document verification on blockchain is an initiative driven by the Ethereum Blockchain, where student documents are stored and governed.

The process of management is end-to-end, including the issue and verification of documents. The issuer, in this case usually an institution, can issue documents for an entity that will use the documents saved on the network to view and verify for authentication and information verification. Blockchain is a decentralized ledger and public network that facilitates secure and transparent transaction capture and confirmation. Its unique features of irreversibility, transparency, and decentralization make it a perfect platform for online document verification. Blockchain can be used to authenticity.

This method offers a better and less costly solution in addition to improving security and reducing chances of fraud and errors through the blocking of fraudulent IDs. Besides verification, the system also has the capability of storing and fetching documents using the Inter Planetary File System (IPFS). The documents are recorded in IPFS, and their hash values are stored.

1.2 MOTIVATION

Legacy document management systems have worked well for decades but are particularly vulnerable today to contemporary risks that blockchain technology shields against. The greatest risk is the potential for data breaches and unauthorized access, which can subsequently provide sensitive information into the hands of malicious parties.

Essentially, standard databases are centralized, and it is this centralization that has created them as vulnerabilities for cyber fraudsters. But this hazard is avoided in Blockchain due to its lack of centralization because of the scattering of data between a group of nodes within a network that renders illegal access complicated and the system increasingly invulnerable.

Spread of counterfeit documents is another serious threat. This has recently become feasible with sophisticated duplication methods. Fake documents are rapidly becoming a concern since the secure storage of genuine documents in databases is quite often wanting. Blockchain technology thus presents a solid solution to this due to its transparency and immutability. Because once a document is placed on blockchain, it is never possible to change or destroy that document since it carries a timestamp with it and will therefore be an auditable history in providing proof of the document's authenticity, making it nearly impossible to produce copies of documents or alter current ones.

The blockchain responds to some major document management challenges by heightening security against intrusions and providing a fool proof method of validating a document's genuineness, thereby guaranteeing integrity and reliability in sensitive data.

1.3.1 Problem Definition

Conventional DMS are faced with great challenges including security vulnerabilities, transparency gaps, inefficiency, and lack of trust. Central storage systems are susceptible to cyber-attacks which expose them to intrusions. Manual inputting and verification of data worsen the situation since it brings with its possibilities of mistakes and inefficiency.

Advancement in complex duplication methods has also led to the widespread of counterfeit documents which in turn reduces the foundations of verification processes for documents. It is transparent, immutable, and decentralized. Blockchain also spreads the data across numerous nodes, providing robust security against unauthorized access attempts and minimizing such risks. Automated smart contracts can indeed make the input and verification of data dependable, clear, and free from human mistakes, thus

making it significantly more efficient. This provides authenticity and integrity in the issue of papers-verifying the very core of the issue in DMS traditionalism.

1.3.2 Proposed work's purpose

The purposes of applying blockchain technology in document verification are to alter the existence, verification, and security of documents. The majority of traditional DMS are not defined by security, efficiency, and an open platform that embodies trust in its interfaces. Blockchain is trusted for decentralized architecture support in terms of making its storage centers and accessibility more secure. Information is spread across nodes within a network, and the system thus keeps unauthorized access and cyber attacks at bay. The sensitive data thus guarded will remain confidential.

Also, the blockchain is tamper-proof; once written, a document cannot be altered or deleted, thereby providing an audit trail that can be verified and ensuring authenticity of documents and against potential forgery of documents since alteration or copying of documents will soon be apparent. Moreover, the use of smart contracts will provide an automated method of data entry and verification thus the likelihood of minimal human error, and efficiency will be highly enhanced.

The ultimate goal is to achieve a document verification process that is simultaneously secure and transparent and efficient and reliable. This will instill confidence in the users in the authenticity and integrity of the documents made available to them and the processes involved in the management and verification of such processes.

1.4.1 Scope of the Project

- Blockchain can be implemented within the automated management systems of individual higher education institutions or groups of educational institution [11]. In education sections, critical of Students' information are vital plus sensitive and to retrieval data of general administrative framework, learning and research may time consuming that cased very problematic [12]
- Designing a decentralized system that leverages blockchain and makes it more secure & transparent. The system has three stakeholders

a) Issuer: The university/college that will issue the academic document
b) Verifier: The party which will be verifying the student's certificate for admission to higher university or employment
c) User: The recently graduated student

- The system eliminates incidences of forged and counterfeit certificates being generated.

1.4.2 Limitations

- No Wallet Recovery Mechanism: In case a user (issuer or stud loses access to his/her crypto wallet, there is no mechanism for recovering or changing ownership of their documents.
- No Bulk Issuing or Verification: The platform does not support bulk operations, so it is not efficient for universities or businesses handling large numbers of documents.
- No Role-Based Access Control: There is no distinction between user roles (e.g., admin and staff), restricting flexibility for big institutions or organizations.
- No Update or Edit Functionality for Certificates: Any error in a certificate (such as a typo) needs to be fully invalidated and reissued. There is no ability to merely edit mistakes.
- Requiring Third-Party Services (IPFS & Ethereum): The system relies extensively on outside services. When IPFS or the Ethereum network experiences problems, users can lose access or experience service outages.

1.5 METHODOLOGIES OF PROBLEM SOLVING

This is a project that seeks to deploy an effective anti-forgery mechanism for documents, including mark sheets, transcripts, diplomas, official identification certificates and other certificates. The intention is to provide assurance of the authenticity of documents, minimizing the occurrence of forging them, and conserving time and financial resources for all parties involved in document verification.

The project's solution is based on three roles or parties: An Issuer, a Verifier, and a User.

- The issuer is the entity that generates and issues the electronic certificate or document
- Verifier is the prospective employer or any individual who wishes to check the authenticity of the certificate presented by the user.
- Lastly, the user is the one receiving the certificate and can only see the documents issued to him/her.

This is a project that offers an effective anti-forgery solution for documents. With the application of a combination of blockchain, IPFS, and hash functions, the authenticity of the certificate can be guaranteed, minimizing the occurrence of fake certificates and saving time and financial resources for all parties involved in document verification.

CHAPTER 2
LITERATURE REVIEW

LITERARTURE REVIEW

2.1 LITERATURE REVIEW

technology has emerged as a robust solution for verifying educational and professional certificates, addressing the longstanding issues of document forgery, inefficiency, and lack of transparency. Traditional methods, which often involve manual verification by third-party entities, are prone to delays and fraud. For instance, paper-based certificates can be easily damaged, lost, or tampered with, leading to challenges in authenticating a candidate's credentials. In educational contexts, institutions can digitally issue certificates, hash them using cryptographic functions, and store these hashes on a blockchain. This method, utilized by projects like the one proposed by Anjali Singh et al., ensures that any attempt to alter the certificate would result in a hash mismatch, making the forgery detectable. The Ethereum blockchain, combined with smart contracts, plays a critical role in automating the verification process. Once a certificate is uploaded and hashed, it is stored on the blockchain alongside a unique transaction ID, which can be referenced for future validation [1].

By leveraging blockchain, these problems can be mitigated through its immutable, decentralized, and transparent nature. In related research, the use of a national eID card for notarization further exemplifies blockchain’s capability in secure document verification. This approach integrates Public Key Infrastructure (PKI) to authenticate the issuer's identity, effectively replacing traditional notary services with automated smart contracts [2].

Blockchain-based DMS also promotes data ownership and transparency, as users control their records and can grant or revoke access as needed. In both SDMS and CDMS, decentralized networks eliminate reliance on a single authority, significantly reducing risks associated with data breaches and unauthorized access. The technology also helps prevent fraud through non-repudiable transaction records, reducing disputes and improving accountability. These blockchain-based solutions, therefore, revolutionize document management by reinforcing security, ensuring transparency, and providing participants with direct control over their data, paving the way for more efficient, scalable, and trust-based digital ecosystems [3].

Document Management System (SDMS) based on Ethereum, blockchain technology safeguards student records by enabling immutable and decentralized storage, which facilitates the prevention of unauthorized document modifications. Smart contracts on the Ethereum blockchain automate verification processes, streamlining operations, and minimizing administrative workload, making the process more reliable and error-free [4].

Additionally, systems like the one developed by Prof. Renuka Vaidya and team focus on document management by combining blockchain with IPFS (Inter Planetary File System), enabling secure, decentralized storage and easy retrieval of documents [5].

Additionally, construction-specific DMS (CDMS) frameworks utilize blockchain and Interplanetary File System (IPFS) storage for managing extensive and complex project documentation, enhancing security by distributing control across participants. In this system, a cryptographic indexing structure and smart contracts are used to establish secure workflows, track document versions, and uphold data consistency, providing a structured yet flexible solution for the unique demands of construction projects [6].

Blockchain-based Decentralized Personal Document Locker, which addresses the need for secure storage without centralized control. It proposes using blockchain to maintain the immutability and integrity of documents. Another work, Distributed Data Sharing System based on Smart contract and IPFS, examines the benefits of using blockchain combined with decentralized storage like IPFS to enhance data security and accessibility. Additionally, other research highlights the role of cryptographic methods like symmetric and asymmetric encryption in ensuring data privacy, confidentiality, and authenticity [7].

2.2 SUMMARY

The "Document Verification and Management System using Blockchain" focuses on addressing the limitations of traditional document management, such as forgery, tampering, and inefficiency. Blockchain’s decentralized ledger ensures data integrity by recording every document-related transaction in a secure, immutable format, where once a document is verified and stored, it cannot be altered or deleted. The system also uses

cryptographic hashing to protect sensitive information while ensuring its authenticity and origin. Smart contracts play a crucial role by automating the verification process, ensuring that predefined conditions are met before granting access or approval, which reduces human intervention and minimizes errors. The integration of digital signatures further strengthens the system's reliability, allowing only authorized individuals to verify or access documents. Blockchain-based document management can be applied across various industries such as education (certificates), healthcare (medical records), legal services (contracts), and finance (audit reports). The system promotes transparency, streamlines workflows, and enhances trust by eliminating the need for intermediaries in document verification processes.

CHAPTER 3
SOFTWARE REQUIREMENTS SPECIFICATION

SOFTWARE REQUIREMENTS SPECIFICATION

3.1 ASSUMPTION AND DEPENDENCIES

Assumptions:

- A reliable and secure blockchain network is available.
- Users are willing to adopt the new system.
- Data recorded on the blockchain is accurate.
- The system complies with legal requirements.
- The system integrates with existing databases.

Dependencies:

- Choice of platform (e.g., Ethereum).
- Development of smart contracts for automation.
- Use of robust cryptographic methods.
- Reliable network for decentralized communication.
- Development of a user-friendly interface.
- Efficient storage solutions for large volumes of data.
- Implementation of strong security protocols.

3.2 FUNCTIONAL REQUIREMENTS

- User Authentication through MetaMask: The system is also integrated with the MetaMask wallet, and the users (Issuer, User, Verifier) can safely authenticate using their personal blockchain address. This way, each user gets uniquely identified and authenticated without a conventional username and password.
- Document Issuance by Issuer: The Issuer can upload and issue certificates to users. The certificate is hashed, given a unique UUID, uploaded to IPFS, and then stored on the Ethereum blockchain along with the recipient's address. This guarantees immutability, traceability, and ownership of issued certificates.
- Decentralized Document Storage via IPFS: Upon release, the certificate is placed on IPFS (InterPlanetary File System), a network for decentralized storage of files. The system creates a content-addressable link (CID/IPFS URL), and the user or verifier can utilize it to download the file securely.

- Document Viewing for User: User can log in to the platform via their MetaMask wallet and see the list of all certificates issued to them. The certificates are displayed with relevant metadata like issuer name, issuance date, IPFS link, UUID, and status (valid/invalid).
- Document Verification for Verifiers: Verifiers (like employers or institutions) can post a digital certificate (e.g., from a user), and the system calculates its hash and checks it with the stored hash on the blockchain. If they match, the certificate is checked as original. Otherwise, it is marked as invalid or altered.

3.3 NON-FUNCTIONAL REQUIREMENTS

- **Usability:** The system is built with current UX/UI practices (React.js + Chakra UI) so that the user experience is seamless and intuitive. All actors — users, verifiers, and issuers must be able to use the platform without extensive training or guidance.
- **Reliability and Availability:** The application has error-recovery features to ensure minimal working capability even under failure. If some module fails (e.g., IPFS access or response from blockchain), the other part of the application must continue to work normally where feasible.
- **Capacity:** The application is based on blockchain and decentralized storage (IPFS) and hence needs considerable memory and computing power, particularly on the server side for transaction processing and handling smart contracts.
- **Maintainability:** The system is developed with SOLID principles and DRY coding methodologies, hence facilitating easier updating, debugging, and scaling in the future. This enhances long-term maintainability through the minimization of technical debt.
- **Security:** Through the employment of the Ethereum blockchain and smart contracts, the system guarantees data integrity, immutability, and controlled access. All the documents are hashed, and the ownership is captured, rendering unauthorized changes virtually impossible.

3.4 SYSTEM REQUIREMENTS

3.4.1 Database Requirements:

The Application stores the entire data about users and certificates issued into the blocks of blockchain

Below Mentioned are the user details stored:

- Name (Issuer/User)
- Wallet Address (Issuer/User)

Below Mentioned are the certificate details stored:

- Name of the certificate
- Wallet Address of Issuer
- Wallet Address of Owner
- UUID (Used to uniquely identify certificate)
- Computed hash of the certificate
- IPFS Link (To access the document stored on IPFS)
- Certificate Status (Valid/Invalid)

3.4.2 Software Requirements:

Frontend - React.js, CSS, HTML, ChakraUI.

- **React.js**

According to our research for building high end user interfaces React is the best option available out there. It is a JavaScript library for building user interfaces. Is used to build single-page applications. allows us to create reusable UI components. It is maintained by Meta (formerly Facebook) and a community of individual developers and companies. The application needs to be more user friendly to let users properly understand the features of the application. React.js has many features which helps in building a user-friendly interface.

also makes it easy for developers to develop UI using many useful features of React. React adheres to the declarative programming paradigm. Developers design views for each state of an application, and React updates and renders components when data changes. This is in contrast with imperative programming.

- **HTML**

HTML is the standard markup language for Web pages. It can be assisted by technologies such as Cascading Style Sheets (CSS) and scripting languages such as JavaScript.

HTML elements are the building blocks of HTML pages. With HTML constructs, images and other objects such as interactive forms may be embedded into the rendered page. HTML provides a means to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists, links, quotes and other items. HTML elements are delineated by tags, written using angle brackets. Tags such as <img /> and <input /> directly introduce content into the page. Other tags such as <p> surround and provide information about document text and may include other tags as sub-elements. Browsers do not display the HTML tags but use them to interpret the content of the page.

- **CSS**

As mentioned above CSS defines the look and layout of content. CSS is the language we use to style an HTML document. CSS describes how HTML elements should be displayed. CSS is designed to enable the separation of presentation and content, including layout, colours, and fonts.[3] This separation can improve content accessibility; provide more flexibility and control in the specification of presentation characteristics; enable multiple web pages to share formatting by specifying the relevant CSS in a separate .css file, which reduces complexity and repetition in the structural content; and enable the .css file to be cached to improve the page load speed between the pages that share the file and its formatting.

As the project requires a little bit of a complex UI, CSS is used as it has a simple syntax and uses a number of English keywords to specify the names of various style properties.

- **Chakra UI**

Chakra UI is a simple, modular and accessible component library that gives you the building blocks you need to build your React applications. [2]

Key features of Chakra UI:

1. Each one of Chakra UI's components are approachable using WAI-ARIA standards.

2.Components are simple to edit, expand, and theme.

3.Components are small and easy to combine to construct larger structures.

4.Switching between other colour modes, such as light and dark, or perhaps any other collection of colours, will be a breeze.

5.Most libraries and frameworks are designed to help you achieve more with less in less time.

6.Although the community is relatively small, it is quite active. [11]

BACKEND: **Solidity, IPFS, HardHat**

- **Solidity**

Solidity is an object-oriented, high-level language for implementing smart contracts. Smart contracts are programs which govern the behaviour of accounts within the Ethereum state. Solidity is a curly-bracket language designed to target the Ethereum Virtual Machine (EVM). It is influenced by C++, Python and JavaScript.

It acts as a tool for creating machine-level code and compiling it on the Ethereum Virtual Machine (EVM). One important reason why Solidity is used for the project is because it has a lot of similarities with C and C++ and is pretty simple to learn and understand. For example, a “main” in C is equivalent to a “contract” in Solidity.

- **IPFS**

As the application is based on blockchain Technology IPFS is used. It is a distributed system for storing and accessing files, websites, applications, and data.

IPFS is a peer-to-peer (p2p) storage network. Content is accessible through peers located anywhere in the world, that might relay information, store it, or do both. IPFS knows how to find what you ask for using its content address rather than its location.

There are three fundamental principles to understanding IPFS:

➔ Unique identification via content addressing

➔ Content linking via directed acyclic graphs (DAGs)

➔ Content discovery via distributed hash tables (DHTs)

- **Hardhat**

Hardhat is a development environment for Ethereum software. It consists of different components for editing, compiling, debugging and deploying your smart contracts and dApps, all of which work together to create a complete development environment. [3]

Hardhat Runner is the main component you interact with when using Hardhat. It's a flexible and extensible task runner that helps you manage and automate the recurring tasks inherent to developing smart contracts and dApps.
Hardhat Runner is designed around the concepts of tasks and plugins. Every time you're running Hardhat from the command-line, you're running a task. For example, npx hardhat compile runs the built-in compile task. Tasks can call other tasks, allowing complex workflows to be defined. Users and plugins can override existing tasks, making those workflows customizable and extendable

3.4.3 Hardware Requirements:

1. **Modern Computer/Laptop**

- In a position to host modern web browsers such as Google Chrome (v80+) or Microsoft Edge.
- Minimum recommended specs:
  Processor: Dual-core CPU (Intel i5 equivalent and above)
  RAM: 8 GB and above
  Storage: 100 GB of free space (to hold project files, IPFS cache, and blockchain simulation data)

2. **Stable Internet Connection**

- Needed for IPFS access, interaction with the Ethereum network, and connection to MetaMask.

3.4 ANALYSIS MODEL

For the project, the Agile SDLC model has been utilized. It was selected because of its adaptability, iterative creation, and constant feedback strategy — all of which fit right into contemporary web and blockchain app development. Following are the features:

- **Iterative Development:** The project was divided into smaller modules like user authentication, certificate issuing, document storing on IPFS, and verification of certificates. Each module was implemented and tested in cycles (sprints).
- **Regular Testing and Feedback:** Once every module was done, they were tested exhaustively, and modifications were implemented based on feedback from peers and mentors.
- **Collaborative Teamwork**: Team members progressed concurrently on frontend, backend, and smart contracts, stitching them together at each iteration.
- **Flexibility:** In development, there were changing requirements — for instance, refining the user interface or dealing with edge cases (i.e., non-conformant documents). With the Agile pattern, such adaptations were smoothly folded in.

CHAPTER 4
SYSTEM DESIGN

SYSTEM DESIGN

4.1 SYSTEM ARCHITECTURE

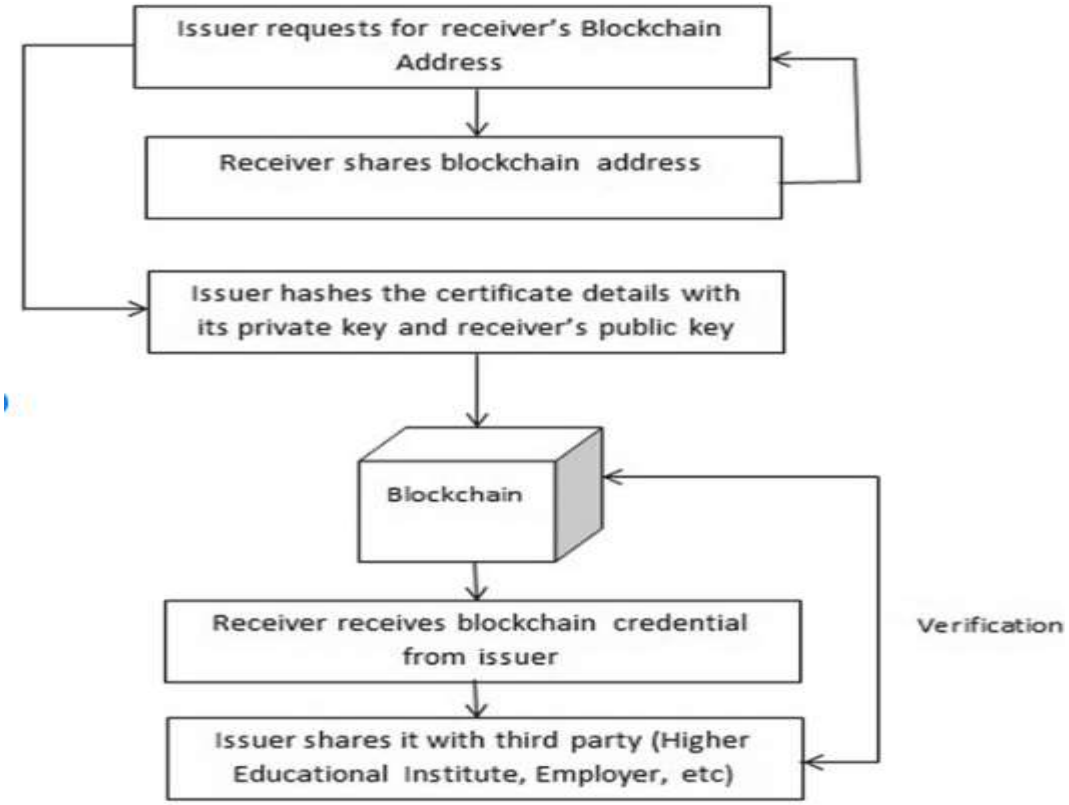

Fig 1. System Architecture

The diagram illustrates the process for issuing and verifying blockchain-based credentials, such as certificates:

1. **Issuer requests the receiver's Blockchain Address**: The process begins with the issuer, who is responsible for creating the credential, requesting the receiver's blockchain address. This address serves as a unique identifier for the receiver on the blockchain network.
2. **Receiver shares blockchain address**: The receiver, who is the intended recipient of the credential, provides their blockchain address to the issuer.

3. **Issuer hashes the certificate details**: The issuer takes the certificate details and hashes them using a combination of their private key and the receiver's public key. This step ensures that the certificate information is securely encoded and tied to both the issuer and the receiver, providing a secure way of associating the credential with both parties.
4. **Data is stored on the Blockchain**: The hashed credential details are then stored on the blockchain. Blockchain acts as a distributed ledger that keeps a permanent, immutable record of the credential, allowing for future verification.
5. **Receiver receives blockchain credential from issuer**: Once the credential is recorded on the blockchain, the receiver can access it from the blockchain, effectively receiving the digital certificate.
6. **Issuer shares it with third party (Higher Educational Institute, Employer, etc.)**: The issuer or receiver can share access to the credential with a third party, such as a higher educational institution, employer, or other verifier. The third party can access the blockchain record to verify the credential's authenticity.
7. **Verification**: The third party verifies the credential by checking the blockchain record. Since the information is hashed and secured by both the issuer's private key and the receiver's public key, this ensures the credential is authentic and tamper-proof.

4.2 MATHEMATICAL MODEL

To express the central functionality of the system — most importantly, document issuance, hashing, storage, and verification — we introduce the following mathematical model:

System Model (S):

Let the system be defined as:

S = {I, P, O, F, DD, NDD}

Where:

- I = Input set
- P = Process set
- O = Output set
- F = Set of functions

- DD = Deterministic Data
- NDD = Non-Deterministic Data

Input (I):

I = {D, UID, WA_u, WA_i}

Where:

- D = Document uploaded (raw file)
- UID = Unique document identifier (UUID)
- WA_u = User's Wallet Address
- WA_i = Issuer's Wallet Address

Process (P):

P = {Hash(D), UploadToIPFS(D), Store(D)}

Where:

- Hash(D) = Calculate hash H of document D
- UploadToIPFS(D) = Deposit D onto IPFS and return link L
- Store(D) = Store {UID, H, WA_s, WA_i, L} on blockchain
- Functions (F):
  F = {IssueCertificate(), VerifyCertificate()}
- IssueCertificate() → Accept inputs I, execute P, and record in blockchain
- VerifyCertificate() → Re-calculates document hash, checks against blockchain entry

Output (O):

O = {Success, Failure}

- Success → Document is valid
- Failure → Document is invalid (hash/UUID mismatch)

Date-Dependent Data (DD):

DD = {Hash values, Wallet addresses, IPFS links, UUIDs}

Non-Date-Dependent Data (NDD):

NDD = {Network latency, IPFS availability, User errors}

4.3 DATA FLOW DIAGRAM:

- Level - 0:

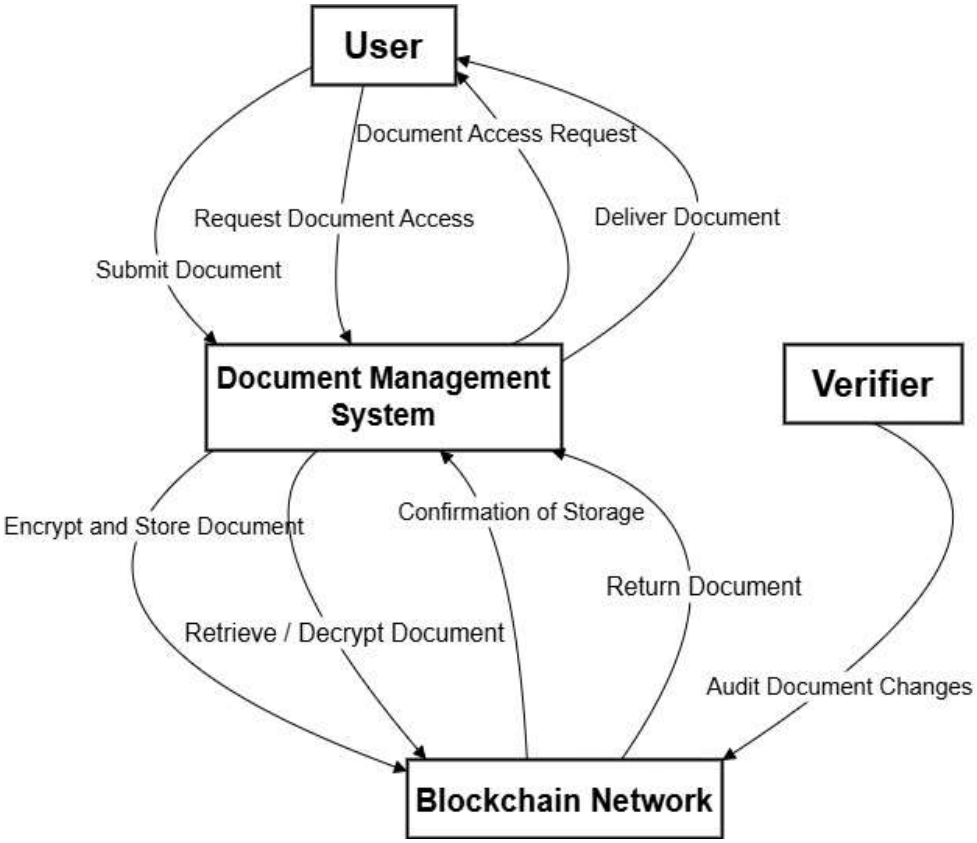

Fig 2. DFD level-0 Diagram

1. **User submits a document:**

- The User sends a document to the Document Management System.
- The system encrypts the document and stores it in a decentralized storage (like IPFS) and sends the hash to the Blockchain Network for verification.

2. **Storing and Confirming Document:**

- The Document Management System receives confirmation of successful storage and recording on the Blockchain Network.

3. **Request Document Access:**

- The User can request access to their documents. The system retrieves and decrypts the document as needed.

4. **Document Verification and Audit:**

- The Verifier requests documents from the Document Management System for auditing.

- The system retrieves the necessary documents, allowing the Verifier to validate their integrity using the records on the Blockchain Network.

➢ Level -1:

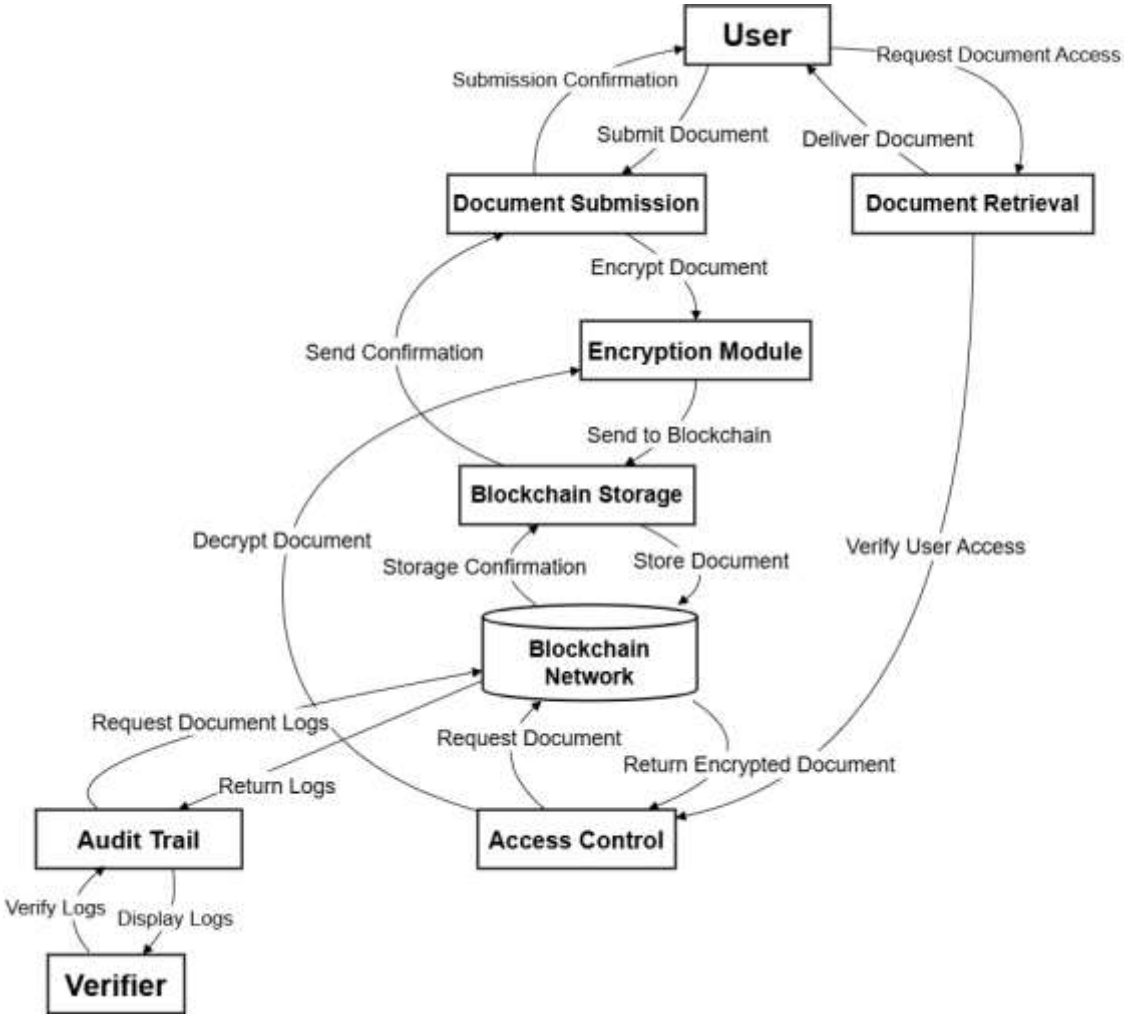

Fig 3. DFD level-1 Diagram

1. **User**: Submits documents for storage and requests access for retrieval.
2. **Document Submission**: Receives documents from the User and sends them to the Encryption Module.
3. **Encryption Module**: Encrypts documents and forwards them to Blockchain Storage, confirming encryption completion.
4. **Blockchain Storage**: Stores encrypted documents in the Blockchain Network and confirms storage.

5. **Blockchain Network**: Main storage layer, returning encrypted documents upon request.
6. **Access Control**: Verifies user access and retrieves encrypted documents for the User.
7. **Audit Trail**: Logs document transactions for transparency.
8. **Verifier**: Reviews logs to ensure process integrity.

- Level - 2:

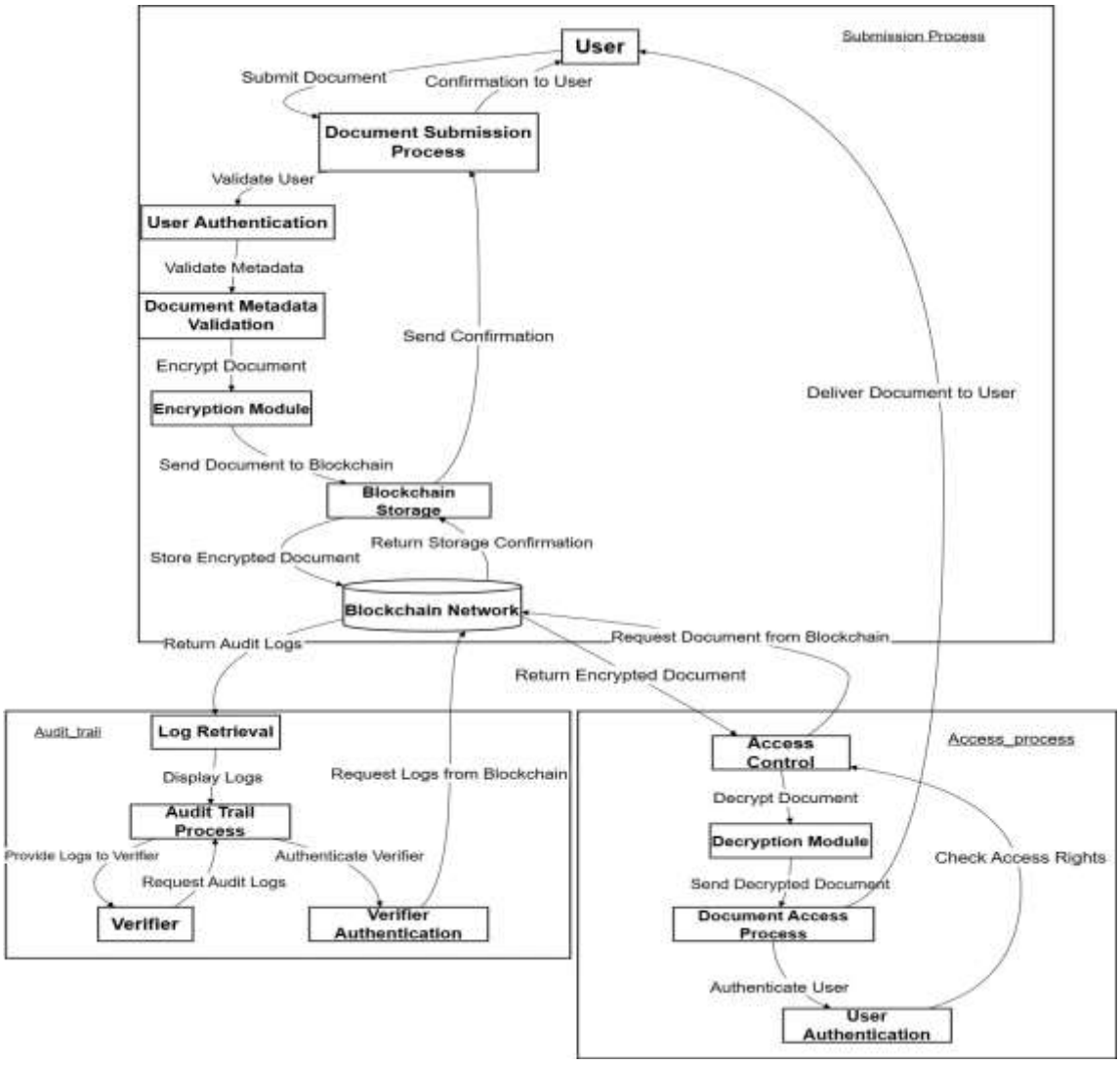

Fig 4. DFD level-2 Diagram

The level-2 details about system with three core processes:

1. **Document Submission**: The User submits a document, which undergoes user authentication and metadata validation. The document is encrypted and stored in the Blockchain Network *via* Blockchain Storage.
2. **Document Access**: Access Control checks user permissions. If authorized, the document is decrypted and delivered back to the User.
3. **Audit Logging**: Logs of document interactions are retrieved from the Blockchain Network, reviewed by an authenticated Verifier to ensure integrity.

4.4 UML DIAGRAM:

- Use Case Diagram:

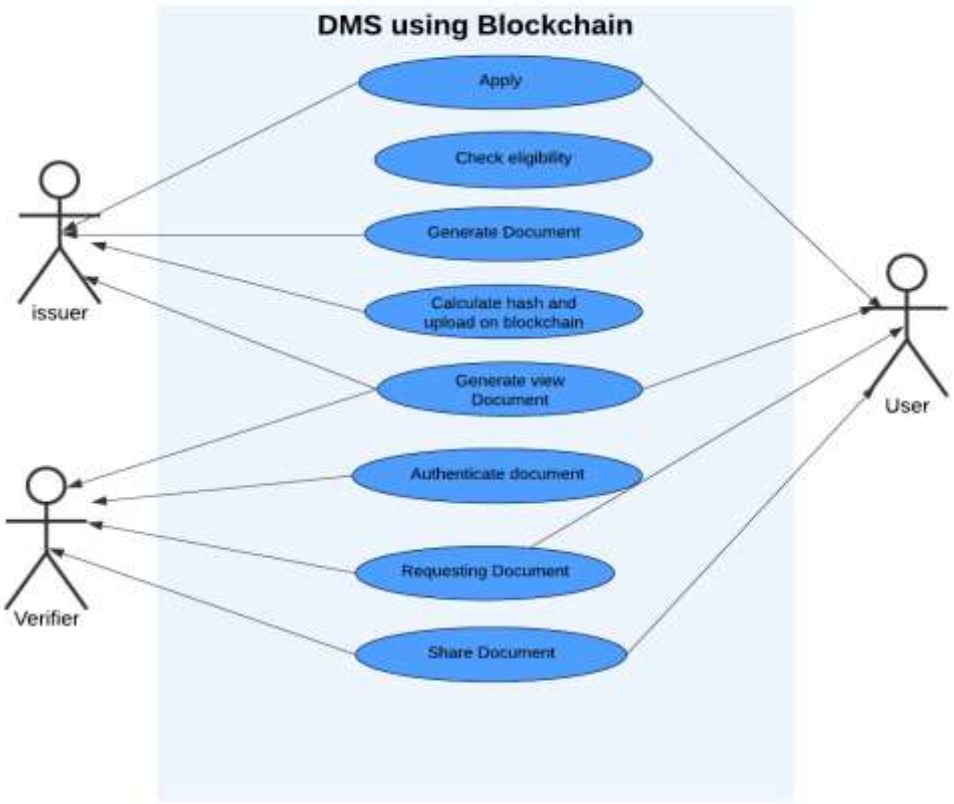

Fig 5. Use Case Diagram

The Use Case Diagram illustrates interactions between different actors and system processes.

Actors:

- **Issuer**: Applies, checks eligibility, generates documents, calculates hash and uploads on blockchain, generates viewable documents, and authenticates them.

- **User**: Interacts by applying, viewing documents, requesting, and sharing documents.
- **Verifier**: Authenticates documents and requests access to them.
  - Sequence Diagram:

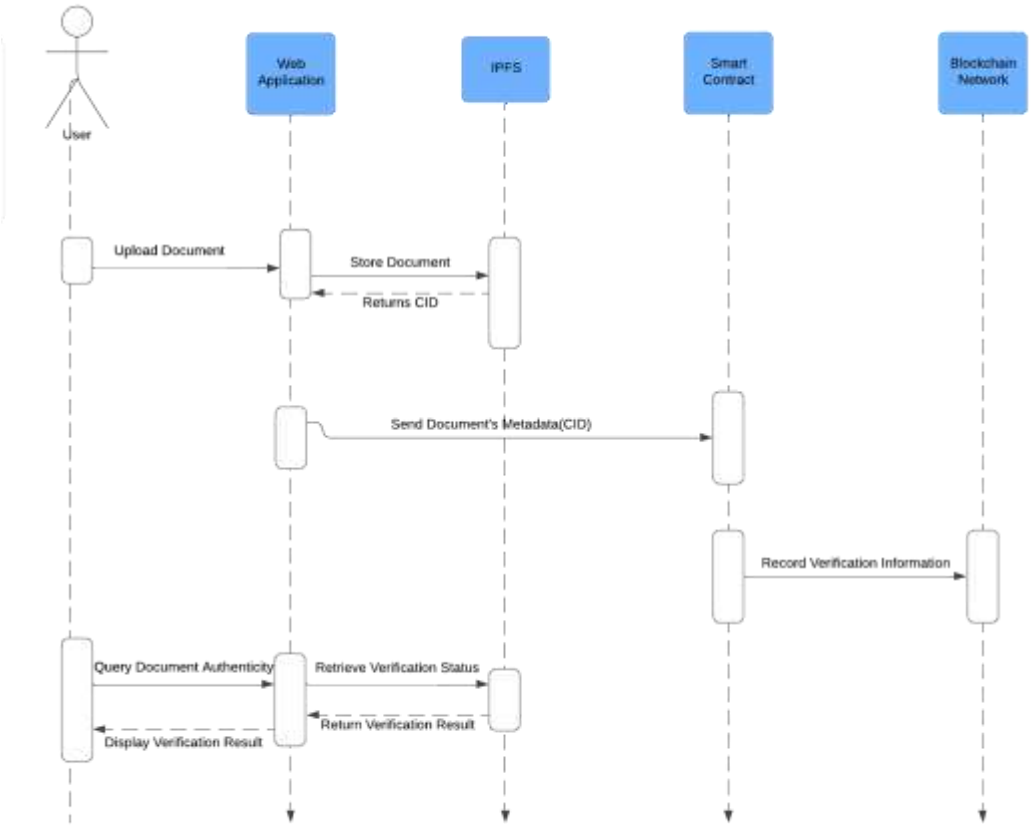

Fig 6. Sequential Diagram

1.Document Upload and Storage:

- Activity: Web Application receives a document from the User and uploads it to the IPFS network.
- Outcome: The document is stored on the IPFS network and a Content Identifier (CID) is generated.

2. Metadata Recording:

- Activity: The Web Application sends the document's metadata (including the CID) to the Smart Contract.
- Outcome: The Smart Contract records the metadata on the Blockchain network.

3. Verification Request:

- Activity: The User queries the Web Application to verify the authenticity of a document.
- Outcome: The Web Application sends a request to the Smart Contract.

4. Verification Retrieval and Display:

- Activity: The Smart Contract retrieves the verification information from the Blockchain and sends it back to the Web Application.
- Outcome: The Web Application displays the verification result to the User.

➢ **Class Diagram:**

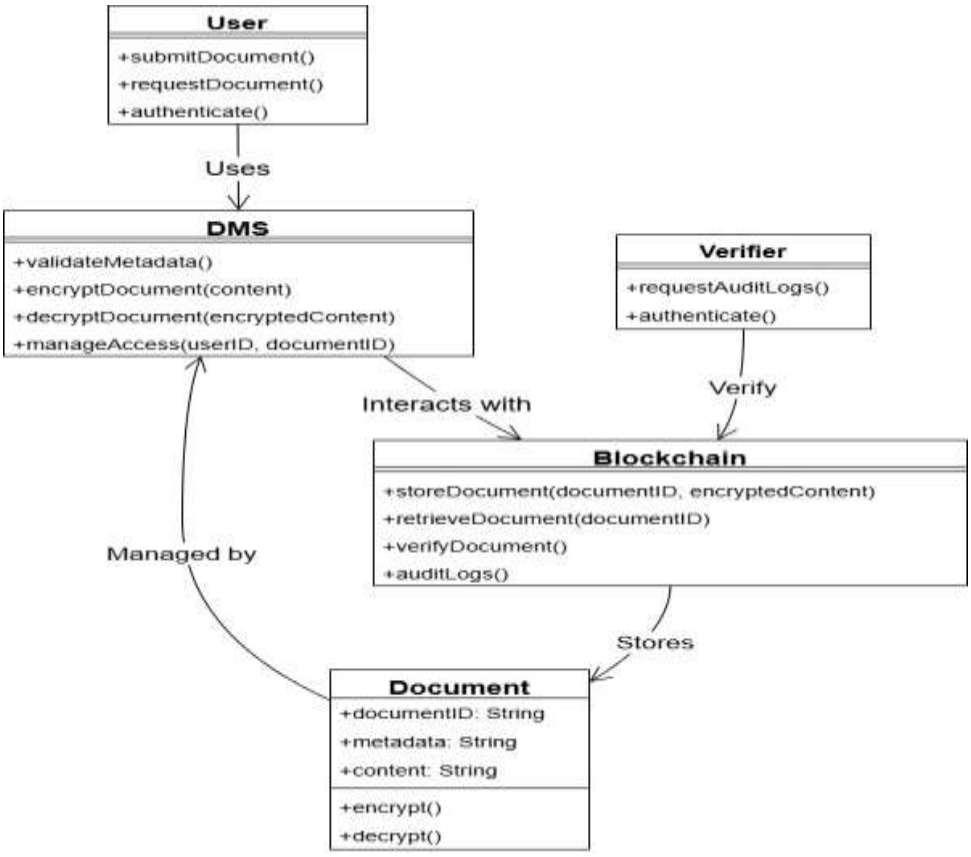

Fig 7. Class Diagram

The Class Diagram illustrates Users can submit and request documents, and verifiers can request audit logs. The Document Management System (DMS) interacts with the blockchain to store and retrieve documents, ensuring their security and integrity. The blockchain also maintains audit logs for transparency and accountability. This system provides a secure and reliable way to manage and verify documents, with the blockchain acting as an immutable record of all transactions.

CHAPTER 5
PROJECT PLAN

PROJECT PLAN

5.1 PROJECT ESTIMATES

Below discussed is a detailed discussion over the project estimates, which are as follows:

5.1.1 Reconciled Estimates

The project is divided into separate phases, each with a corresponding time and effort estimate. After thorough examination of scope, complexity, and interdependencies, the team reconciled the estimated efforts as per the following:

Phase	**Estimated Duration**	**Effort (person-weeks)**
Requirement & Research	July–August 2024	3
Design & Architecture	September 2024	2
Development & Integration	October 2024 – January 2025	8
Testing & Optimization	February 2025	4
Documentation & Submission	March–April 2025	2
Total	**July 2024 – April 2025**	**19 person-weeks**

Table 1: Project Estimates

Each team member contributed collaboratively, rotating responsibilities to enhance learning and ensure quality output.

5.1.2 Project Resources

- **Software Tools**:
  - React.js, Chakra UI (Frontend)
  - Solidity, Hardhat (Smart Contract Development)
  - Node.js, IPFS, MetaMask, VS Code
- **Hardware Requirements**:
  - Personal laptops with ≥8 GB RAM
  - Stable internet connection
  - Web browser supporting MetaMask

5.2 RISK MANAGEMENT

5.2.1 Risk Identification

Risk Description	Type
Blockchain transaction failures	Technical
Loss of MetaMask access by users	Operational
Tool version mismatches (npm, Node.js)	Technical
Academic schedule conflicts (exams)	Human/Resource
IPFS document unavailability	Infrastructure

Table 2: Risk Identification

5.2.2 Risk Analysis

- High Risk: Wallet or smart contract access problems
- Medium Risk: Version clashes or unanticipated bugs
- Low Risk: Availability of team members owing to external commitments

5.2.3 Overview of Risk Mitigation, Monitoring, and Management

- Keep wallet credentials safely backed up
- Pin files on IPFS for enhanced reliability
- Test with Hardhat local blockchain to minimize reliance on public chains
- Schedule adaptive work sessions during peak academic load
- Weekly team reviews to identify and resolve blockers in time

5.3 PROJECT SCHEDULE

5.3.1 Project Task Set

Phase	Tasks Included
Requirement Analysis	Understand roles, gather inputs, set objectives
Research	Study domain (Blockchain, IPFS), evaluate existing systems
Design	Draft system architecture, flow diagrams, and UI prototypes
Development	Build frontend, smart contracts, and backend logic
Integration	Connect components (React + IPFS + Blockchain)
Testing	Validate functions, fix bugs, simulate user interactions
Documentation	Prepare detailed report and user manual
Submission	Final review, submission and viva preparation

Table 3: Project Task Set

5.3.2 Task Network

- Task flow in a semi-linear fashion:
  Research → Design → Development (Frontend + Contracts in parallel) → Integration → Testing → Documentation → Submission
- Some activities like frontend and backend development can occur concurrently to optimize time.

5.3.3 Timeline Chart

A Gantt chart representation is also created for better understanding

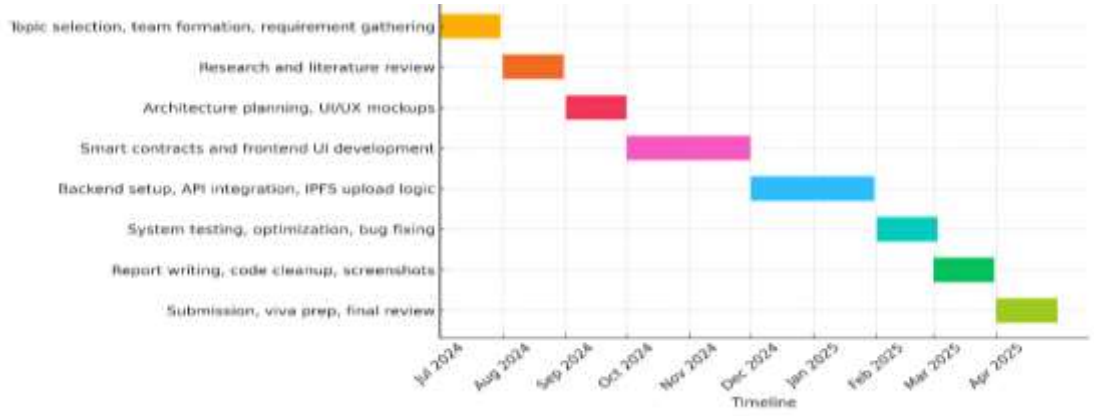

Fig 8. Gantt Chart

5.4 TEAM ORGANIZATION

5.4.1 Team Structure

The project team follows a flat collaborative structure where responsibilities are shared but divided based on strengths and interests.

Member	Primary Role
Gaytri	Backend Developing (Solidity, IPFS, Smart Contracts)
Nidhi	Frontend Developing (React, Chakra UI) and Documentation
Tiya	Frontend Developing (React, Chakra UI) Tester, Documentation & Report Writing

Table 4: Team Structure

Each member contributes to design decisions, testing, and integration to ensure full ownership and understanding of the project.

5.4.2 Management Reporting & Communication

- **Weekly Meetings**: Virtual meet every Sunday for progress updates
- **Task Tracking**: Updating the Gantt Chart
- **Communication Tools**: WhatsApp group for daily sync, Google Meet for demo/testing reviews
- **Documentation**: Shared Google Docs.

CHAPTER 6
PROJECT IMPLEMENTATION

PROJECT IMPLEMENTATION

6.1 OVERVIEW OF PROJECT MODULES

The project's authentication system is modular and has various components, each of which deals with a specific functionality. Each module communicates in a harmonious order to facilitate a secure, decentralized document management and verification system.

1. **Authentication Module**

- Purpose: Verifies the users based on their MetaMask wallet.
- Functionality:

  Facilitates secure login for all three roles: Issuer, User, Verifier.

  Accesses Ethereum wallet to retrieve the public address of the user.

  Verifies role (issuer/user/verifier) based on registered blockchain data.

2. **Issuer Module**

- Purpose: Makes it possible for universities or other institutions to issue documents to users.
- Functionality:

  Uploads raw documents (certificates).

  Creates a unique identifier (UUID) and calculates document hash.

  Uploads document to IPFS and stores metadata (UUID, hash, IPFS link, addresses) on the blockchain.

  Can flag a certificate as invalid in case of incorrect issuance.

3. **User Module**

- Purpose: Enables users to see and share their issued documents.
- Functionality:

  Sees all documents sent to their Ethereum address.

  Sees certificates through IPFS links.

  Sends documents to verifiers with hash, UUID, and public address.

  Notified if any certificate is revoked.

4. **Storage Module (IPFS)**

- Purpose: Stores the actual document files decentrally and securely.

- Functionality:

  Files are stored on IPFS (InterPlanetary File System), providing tamper-proof decentralized storage.

  Each document is retrievable through a distinct IPFS hash.

  Decreases dependency on centralized storage services such as conventional cloud providers.

5. Verification Module

- Purpose: Enables verifiers (e.g., institutions, employers) to confirm document authenticity.
- Functionality:

  Uploads the document received and calculates its hash.

  Cross-verifies it against the blockchain information (hash, UUID, issuer wallet address, user wallet address).

  Returns the outcome as "Valid" or "Invalid" along with appropriate messages.

6. Smart Contract Module

- Purpose: Responsible for all operations involving document issuance and verification on the Ethereum blockchain.
- Functionality:

  Stores hashes, UUIDs, and wallet addresses.

  Offers functions for issuing, validating, and revoking certificates.

  Guarantees immutability and safety through Solidity code.

6.2 TOOLS AND TECHNOLOGIES USED

- React.js: Utilized to create the dynamic and component-oriented frontend interface for all user types (user, issuer, verifier).
- Chakra UI: A new UI library that was utilized to create accessible and responsive interfaces with pre-fabricated React components.
- HTML, CSS, and JavaScript (ES6): Applied to webpage structuring, styles, and interactive functionalities.

- Node.js & Express.js: Backend technologies employed to develop server-side APIs and facilitate communication between the frontend, blockchain, and IPFS.
- Solidity: Programming language for coding Ethereum smart contracts that issue and verify certificates on the blockchain.
- Hardhat: Smart contract development environment for compiling, testing, and deploying smart contracts to the Ethereum network.
- IPFS (InterPlanetary File System): Decentralized file storage system to store certificates securely and permanently.
- MetaMask: Browser wallet extension for secure login, blockchain transaction signing, and identity authentication using wallet addresses.
- Ethereum (Local Network/Testnet): The blockchain system utilized to launch smart contracts and securely store document metadata.
- Visual Studio Code (VS Code): The main code editor utilized to write frontend, backend, and smart contract code.
- Git & GitHub: Collaborative development version control tools for tracking changes, sharing code with team members, and keeping record of changes made.
- Google Docs & Google Sheets: Utilized for planning, writing documentation, and team collaboration management.

6.3 ALGORITHM

While the system is generally powered by web and smart contract technologies, a number of logical algorithms have been incorporated in the system for secure document issuance and verification. The most important algorithms employed are the following:

1. **Document Hashing Algorithm**

- Function: To represent the document uniquely with an immutably digital fingerprint.
- Process:

  Append the document contents with its produced UUID (Unique User Identifier).

  Use a SHA-256 or keccak256 hash function (through Solidity or Node.js) to create a hash.

  Save the resulting hash to the blockchain for later verification.

2. **Certificate Issuance Algorithm (Smart Contract)**

- Purpose: To issue a new certificate onto the blockchain.
- Steps:

  Accept input: user address, certificate hash, UUID, IPFS link.

  Store the certificate information in a smart contract mapping with a status of valid.

  Emit an event indicating successful issuance.

  Implemented in: Solidity smart contract.

3. Document Verification Algorithm

- Purpose: To check if a document uploaded by a user is genuine.
- Steps:

  Input the uploaded document, retrieve its UUID, user address, issuer address.

  Hash the uploaded document with the same hash function.

  Get the matching stored hash and metadata from the blockchain.

  Compare:

    Input hash vs stored hash

    UUID, issuer address, and user address

  Return true if all match and certificate status is valid; otherwise return false.

4. Certificate Invalidation Algorithm

- Function: To flag a previously issued certificate as invalid (e.g., in event of error).
- Steps:

  Take in the UUID and issuer address.

  Verify if the sender is the original issuer.

  Set the certificate's status to invalid from valid.

  Emit an event for tracking.

CHAPTER 7
SOFTWARE TESTING

SOFTWARE TESTING

7.1 TYPE OF TESTING

The project went through several levels of testing to validate reliability, correctness, and security throughout the whole system. The following are the types of testing performed:

1. **Unit Testing**
- Directed towards testing single functions in the smart contracts and backend API.
- Verified that each function such as certificate issuance, verification, and revocation functioned as desired.
- Performed with Hardhat to utilize its in-built testing framework for Solidity.

2. **Integration Testing**
- Confirmed the frontend, backend, smart contracts, and IPFS integrated seamlessly
- Ran actions such as issuing a document from the frontend and validating whether it gets properly hashed, stored in IPFS, and recorded on the blockchain.

3. **Functional Testing**
- Verified system functionalities against specifications — role-based login, viewing of a document, and verification.
- Confirmed each user (Issuer, User, Verifier) could only access desired functionalities.

4. **User Interface (UI) Testing**
- Verified that the layout of the application was consistent and responsive in all browsers (Chrome, Edge).
- Verified that buttons, links, modals, and forms worked properly.

5. **Negative Testing**
- Confirmed that the system responded well to invalid inputs (e.g., invalid documents, incorrect wallet address) without crashing.
- Tested certificate verification using tampered files to ensure rejection.

7.2 TEST CASES AND RESULT

Below are key test cases executed during testing:

Test Case Description	Input / Action	Expected Result	Actual Result
Certificate Issuance	User wallet address, raw document	Certificate is issued and reflected on blockchain	Passed
Document Verification with Valid File	Original certificate file	Verification successful, marked as valid	Passed
Document Verification with Tampered File	Modified version of certificate	Verification fails	Passed
Certificate Invalidation	Issuer invalidates a certificate	Certificate marked as invalid in system	Passed
Access Control	Verifier tries to issue certificate	Action denied due to permissions	Passed

Table 5: Test Cases and Results

CHAPTER 8
RESULTS

RESULTS

8.1 OUTCOMES

The project has been able to fulfil its core mission: creating a secure, decentralized, and tamper-proof platform for issuing and authenticating documents on the Ethereum blockchain and IPFS.

By integrating smart contracts, decentralized storage, and identity management based on wallets, the system minimizes the possibility of tampering with forged certificates and decreases the effort and time involved in verification. By being a role-based platform for Issuers (institutions etc.), Users, and Verifiers (employers or institutions), It provides transparency, trust, and ease of use during the document lifecycle.

The platform:

- Allows institutions to issue verifiable certificates on the blockchain directly.
- Enables users to store and share their documents safely.
- Enables verifiers to verify documents in real time without middlemen.

Features have all been implemented, tested, and proven to work successfully. Utilizing state-of-the-art web technologies (React, Chakra UI), contract logic (Solidity), and distributed tools (IPFS, MetaMask, Hardhat) has yielded a functional prototype that is stable, easy to use, and scalable.

This project not just proves the functionality of blockchain within the documentation community but also gives way to enhanced features like issuing certificates in bulk, multiple-language support, and interfacing with national academic data bases.

Ultimately, it is a proof-of-concept for a new-generation system of document management — secure, efficient, and future-proofed.

8.2 SCREENSHOTS

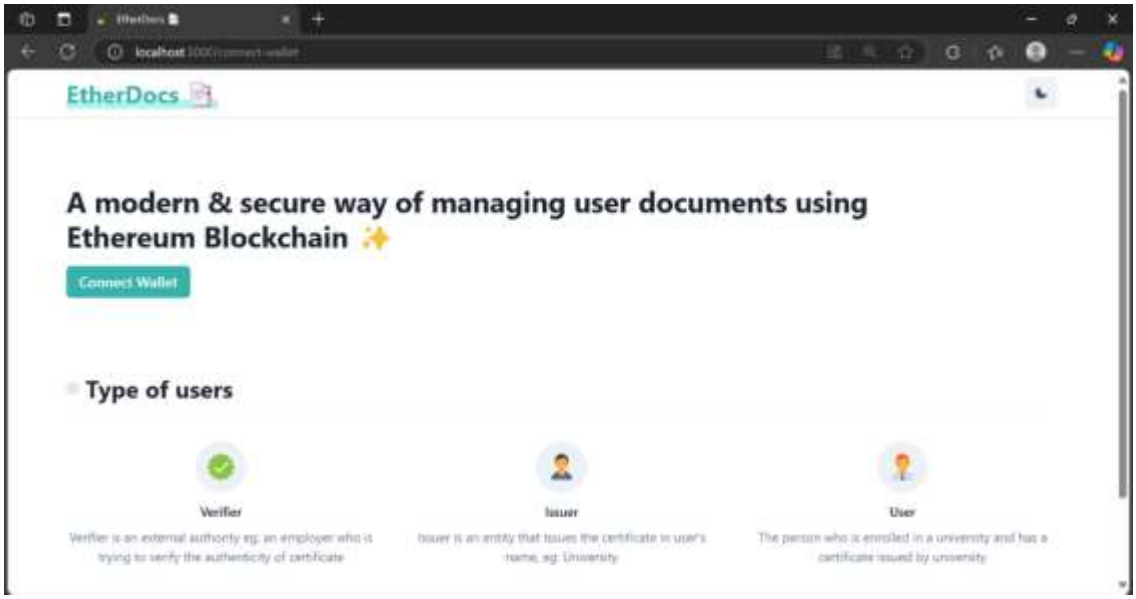

Fig 9. Homepage describing the 3 roles: Issuer, Verifier & User

As shown in Fig, the system revolves around three key roles or entities: the issuer, the verifier, and the user. The issuer, typically a university or other institution, creates an electronic version of the certificate to be issued, along with a unique UUID printed on the document, and a hash value of the document. The certificate is uploaded to the InterPlanetary File System (IPFS), and all data related to the certificate and IPFS link along with the hash value of document is stored on the blockchain. The verifier, typically a potential employer or other interested party, can verify the authenticity of the document by comparing the hash value of the document with the hash value stored on the blockchain. The user can only view the documents issued to them.

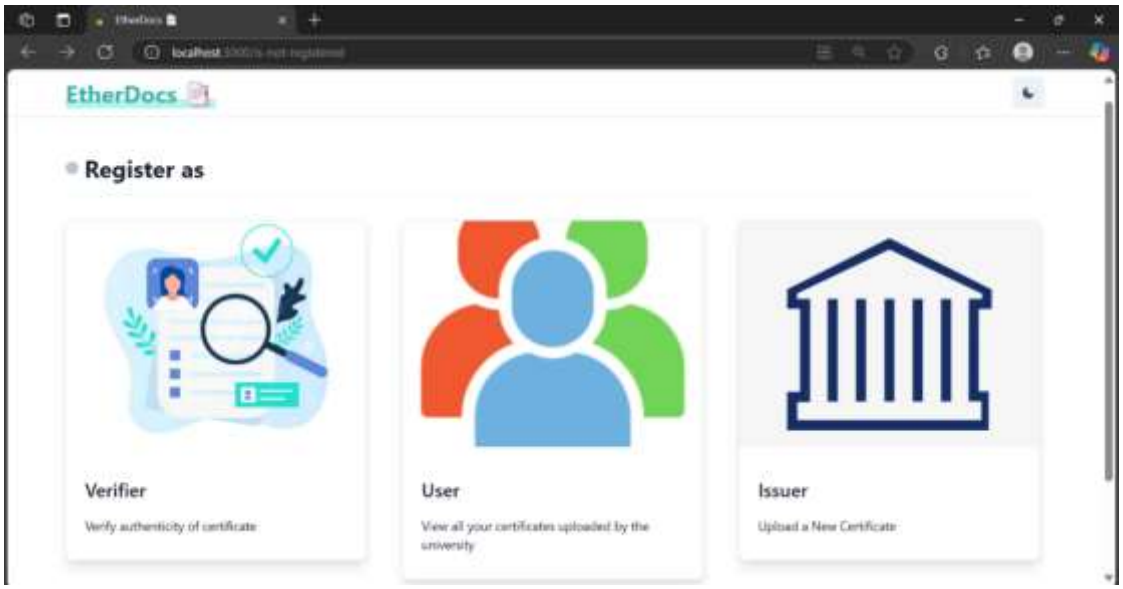

Figure 10. Choosing the role

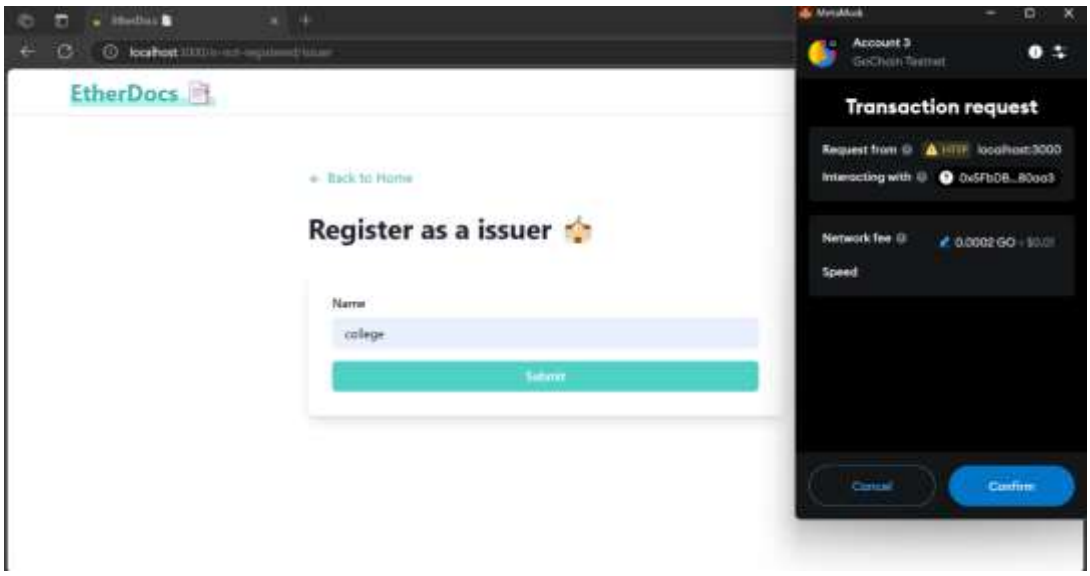

Fig 11. Registering new issuer

The process starts with the issuer creating an electronic version of the certificate to be issued. The electronic version of the certificate contains a hash value of the document, a unique UUID printed on the document. The hash value of the document is a unique digital fingerprint that is generated using a hash function. The UUID is a unique identifier that is assigned to the certificate, and the IPFS link is used to access the certificate on IPFS, a distributed file system.

Once the certificate is created, it is uploaded to IPFS, where it can be accessed by the user. All the data related to the certificate and the IPFS link are stored on the

blockchain. The blockchain is a distributed ledger that is tamper-proof and immutable, making it an ideal platform for storing data that needs to be secured.

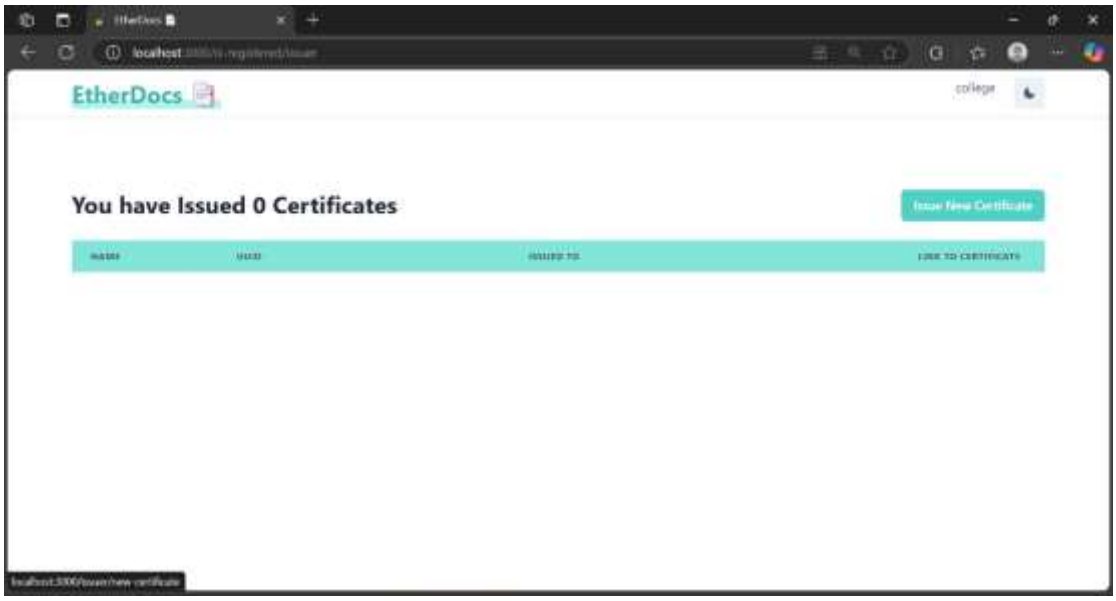

Figure 12. Home Page of issuer

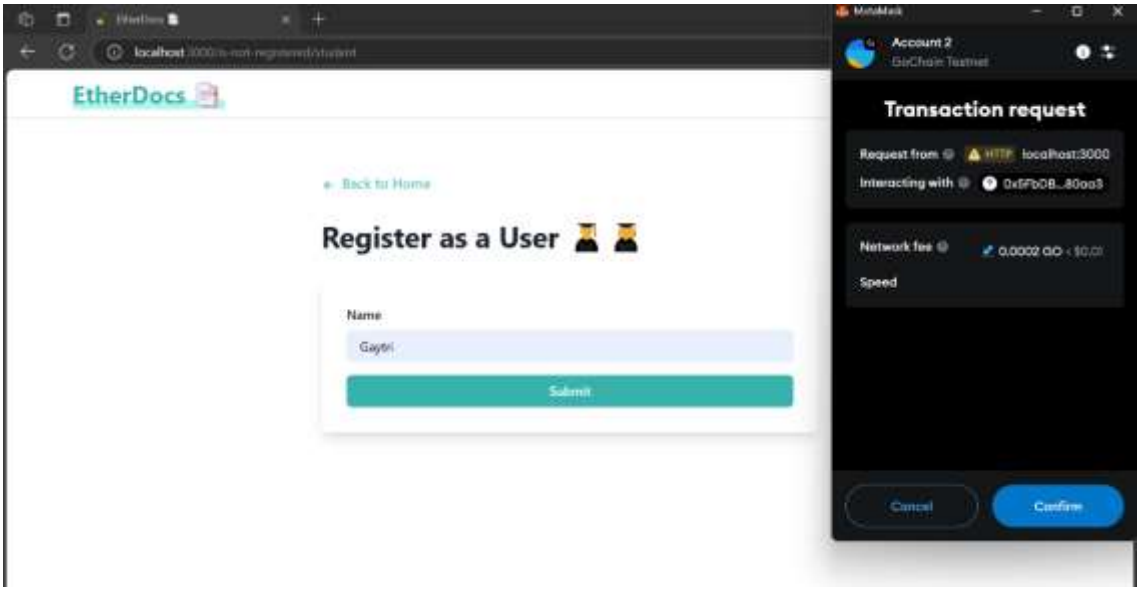

Fig 13. registering new user

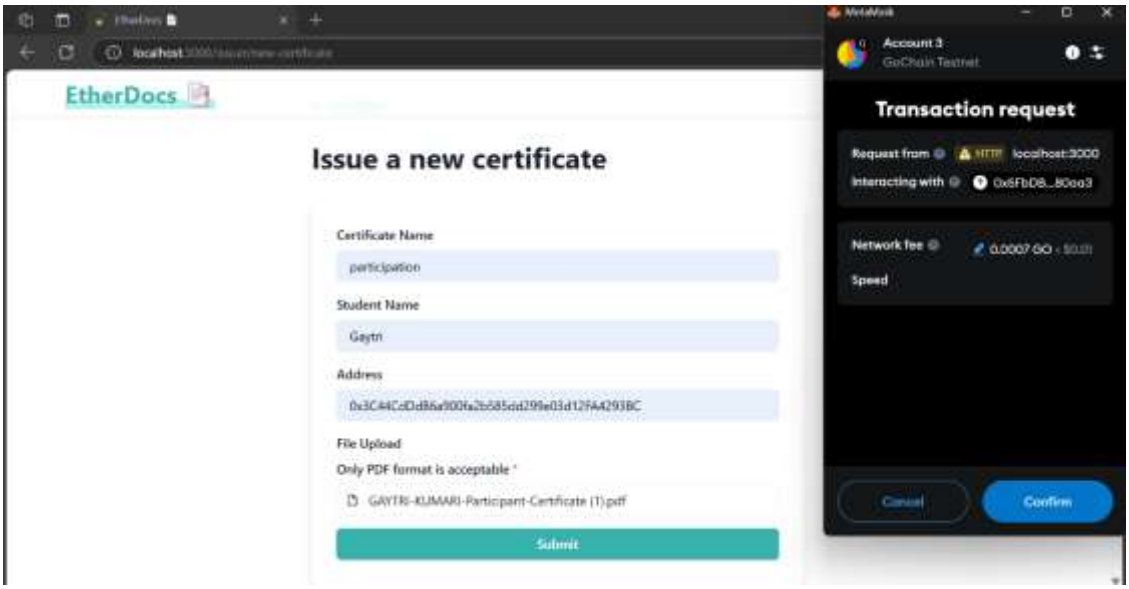

Fig 14. Issuing Certificate for the user

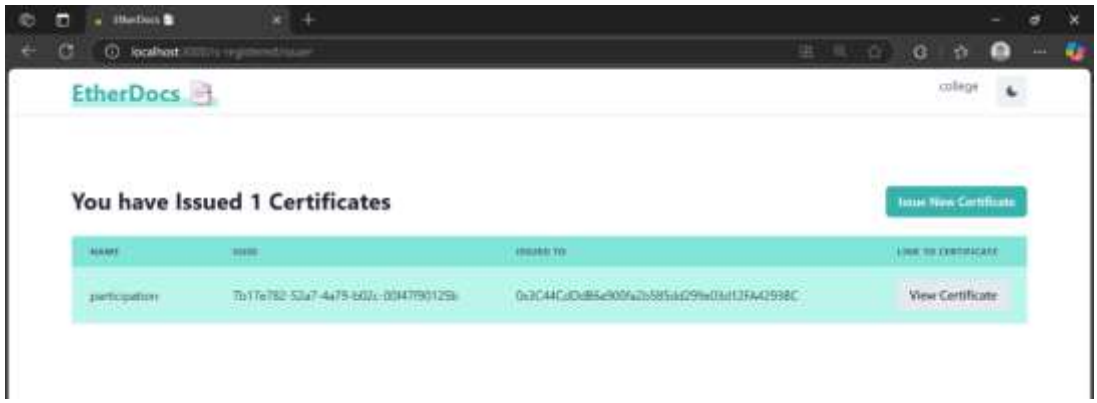

Fig 15. Home Page of issuer After certificate was issued

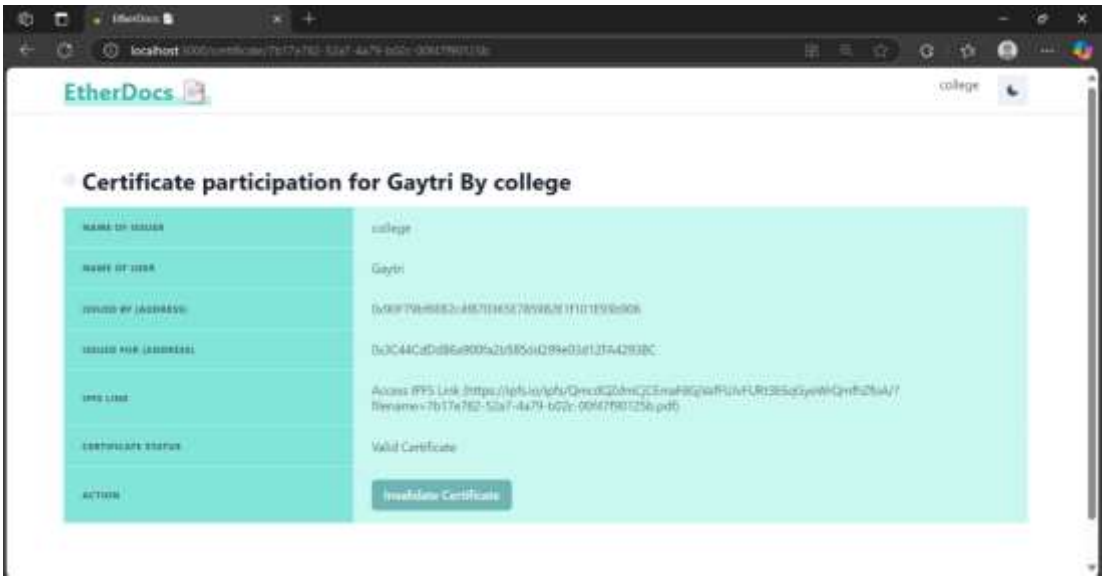

Fig 16. Certificate detail page of issuer with feature to Invalidate Certificate

Fig 17. Issued Ceritificate on IPFS with UUID

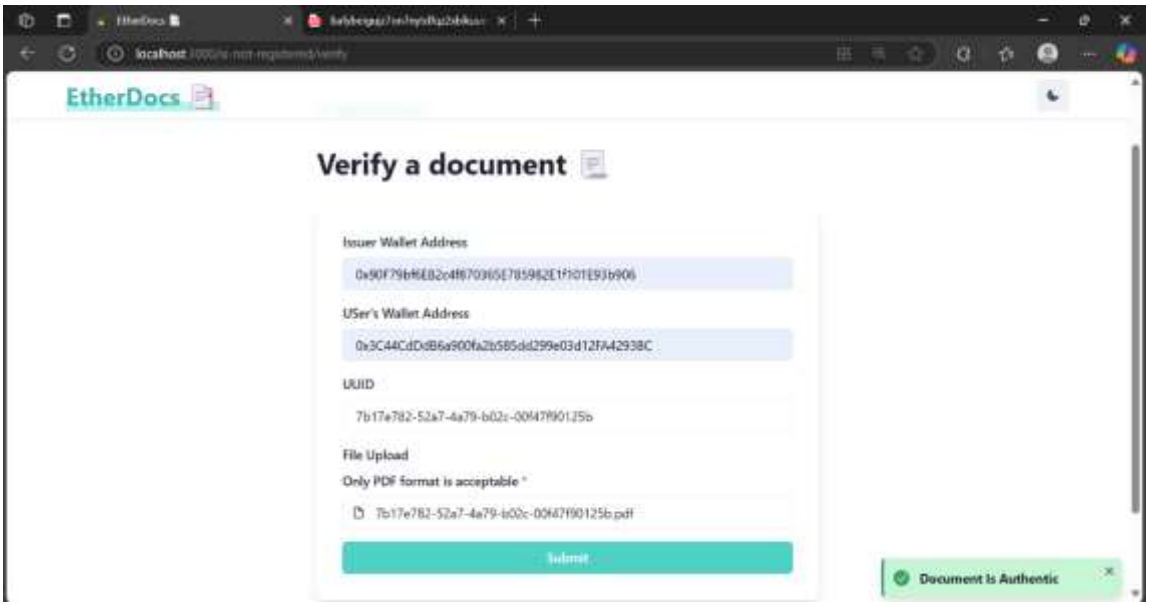

Fig 18. Verification of Certificate at the Verifier's end

In summary, the solution, this a project that provides an efficient anti-forgery mechanism for documents. By using a combination of blockchain, IPFS, and hash functions, the authenticity of the certificate can be ensured, reducing the incidence of counterfeit certificates and saving time and financial resources for all parties involved in document verification. This proposed solution has been implemented successfully.

CHAPTER 9
CONCLUSIONS

CONCLUSIONS

9.1 CONCLUSIONS

The proposed system addresses the major challenges faced in traditional methods of certificate issuance, verification, and storage by leveraging the benefits of blockchain technology. It introduces a robust, tamper-proof mechanism for handling digital certificates, ensuring features such as immutability**,** decentralization, and enhanced security without the need for third-party intermediaries. The system effectively eliminates the risk of fraudulent certificates by utilizing blockchain's transparent and traceable ledger, where each transaction related to certificate issuance and verification is permanently recorded. This traceability makes it easy to verify the authenticity of any certificate. Moreover, the system is significantly faster than traditional methods that rely on paper-based certificates, reducing delays in verification processes. A key innovation is the use of Inter Planetary File System (IPFS**)** for distributed document storage, ensuring that certificates are stored securely across a decentralized network rather than in centralized databases, which are vulnerable to single points of failure. Blockchain technology generates unique hash values for each e-certificate, which are used during the verification process. These hash values act as digital fingerprints, ensuring that the certificates are secure, tamper-proof, and impossible to forge**.**

9.2 FUTURE WORK

Although project has successfully proved the viability of blockchain-based management of documents, there are a number of areas for future development and growth to make the system more scalable, robust, and user-friendly.

One of the key areas of enhancement is the provision of bulk certificate issuance. At the moment, certificates are issued one by one, which might not be efficient for big institutions dealing with thousands of records. Including a bulk upload and issuing facility would make a big difference in terms of efficiency.

Also, the project can be extended to facilitate integration with national frameworks like DigiLocker or the Academic Bank of Credits. This would facilitate wider adoption and enable recognition of certificates across platforms, thus fostering trust and diminishing verification barriers.

For enhanced user experience, the addition of a filtering and categorization feature may be included. This would make it convenient for users and verifiers to view multiple documents on the basis of type (such as transcripts, degree certificates, internship letters) or issue date.

Security and equity may be increased by adding a dispute resolution module wherein a user may appeal in case a certificate is validly invalidated. A structured review process under the direction of the issuing institution would enhance the transparency and credibility of the system.

Additionally, creating a mobile app would improve accessibility, particularly for those in rural or distant locations who might not have access to desktops or laptops. A mobile app could mirror the essential functionality of the platform in a more mobile format.

Additional improvements that can be considered are:

- Role-based permissions within institutions (e.g., admin, issuer, reviewer).
- Analytics dashboard for issuers to monitor certificate activity and verification trends.

In summary, by deploying these enhancements, Project has the potential to grow from a functional prototype into an effective real-world application with the ability to handle large-scale institutions, streamline processes, and verify document authenticity at scale.

9.3 APPLICATIONS

This a general-purpose platform for safe, decentralized document management and authentication. Its use cases go beyond academia to professional, governmental, and international spaces.

- Digital Document Issuance: Organizations can issue significant documents (certificates, IDs, licenses) directly to end-users on the blockchain, minimizing paperwork and fraud.
- Tamper-Proof Record Storage End-users can securely store sensitive documents (agreements, contracts, certifications) in an immutable form using IPFS and blockchain.

- Instant Document Verification: Third parties (agencies, institutions, employers) are able to instantly confirm document authenticity without manual verification.
- Government & Legal Use Cases: Perfect for issuing official records, legal notices, permits, and licenses where transparency and tamper-resistance are paramount.
- Cross-Border Document Sharing: Users can exchange authenticated digital records across borders for work, education, or migration without delay or translation of physical documents.
- Secure Document Sharing in Enterprises: Firms can leverage the platform for internal certification (training, compliance) and securely manage employee credentials.
- Decentralized Identity & Trust Layer: It can be built out as a base for self-sovereign identity (SSI), allowing users to own and manage their digital documents.

REFERENCES

[1] Anjali Singh, SPS Chauhan, Amit Kumar Goel Professor, School of Computing Science and Engineering, Galgotias University Greater Noida, India, "Blockchain Based Verification of Educational and Professional Certificates",2023, DOI: 10.1109/ICCSC56913.2023.10143008

[2] SHINYA HAGA AND KAZUMASA OMOTE Faculty of Engineering, Information and Systems, University of Tsukuba, Tsukuba 305-8577, Japan, "Blockchain-Based Autonomous Notarization System Using National eID Card " ,2022, DOI 10.1109/ACCESS.2022.3199744

[3] Mr. S. CHOUDAIAH, Mr. U. CHANDRASELHAR, Dept of MCA, SVEC - Sree Vidyanikethan Engineering College, Tirupati, "Block Chain Based Document Management System", Vol 12, Issue 08, August/2021 ISSN NO:0377-9254

[4] Yerramsetti Sri Uday Kiran Sai Mahesh, Velagapudi Rohith, Vennam Srinivas Reddy , Mrs B. Ratnamala, Dr. Reddyvaari Venkateswara Reddy, "A review on Student Document Management System based on Ethereum Blockchain (PERSONAL- D)", ISSN: 2278-0181 Vol. 12 Issue 08, August-2023

[5] Prof. Renuka Vaidya, Ms. Sanskriti Punde, Mr. Kartikey Yadav, Mr. Chakradhar Ghute, Ms. Namrata Shinde Assistant Professor, Department of Information Technology Students, Department of Information Technology Sinhgad College of Engineering, Pune, India, "Document Management System using Blockchain", Volume 3, Issue 13, May 2023, DOI: 10.48175/568

[6] Moumita Das, Jack C. P. Cheng, Xingyu Tao, "A Secure and Distributed Construction Document Management System Using Blockchain", January 2021 DOI: 10.1007/978-3-030-51295-8_59

[7] Sakshi Jha, Govind Dhingra, Gagan Mittal, Harsh Vardan, Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India ,"Secured Document Storing Using Blockchain", 2022 IJRTI, Volume 7, Issue 5, ISSN: 2456-3315

[8] Qurotul Aini, Eka Purnama Harahap, Nuke Puji Lestari Santoso, Siti Nurindah Sari, Po Abas Sunarya, University of Raharja, Tangerang, Indonesia," Blockchain Based Certificate Verification System Management", Vol. 7, No. 3, 2023, pp. 1∼10,E-ISSN: 2622-6804 P-ISSN: 2622-6812, DOI: 10.34306

[9] Isyak Meirobiea, Agustinus Purna Irawanb, Husni Teja Sukmanac, Diana Putri Lazirkhad, Nuke Puji Lestari Santoso, Tarumanagara University, Letjen S. Parman Street No. 1, Jakarta 11440, Indonesia," Framework Authentication e-document using Blockchain

Technology on the Government system", International Journal of Artificial Intelegence Research ISSN: 2579-7298,Vol 6, No 2, December 2022

[10] Xue Zhai, Shanchen Pang, Min Wang ,Sibo Qiao ,Zhihan Lv," TVS: a trusted verification scheme for office documents based on blockchain", Complex & Intelligent Systems, https://doi.org/10.1007/s40747-021-00617-1, 3 December 2021.

[11] V.A. Toblatoy, "Using Blockchain Technology for Lerarning", vol. 61, no. 1, pp. 110–113, 2018.

[12] F. O. Ezeudu, N. M. Eya, and H. I. Nworgi, "Application of Blockchain-based Technology in Chemistry Education Students" Data Management', Int. J. Database Theory Appl., vol. 11, no. 2, pp. 11–22, 2018.

APPENDIX

APPENDIX A

Review Paper Certificate:


Certificate of Publication
INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS | ISSN: 2320 - 2882
An International Open Access, Peer-reviewed, Refereed Journal
The Board of
International Journal of Creative Research Thoughts
Is hereby awarding this certificate to
Tiya Mukherjee
In recognition of the publication of the paper entitled
Document Verification And Management System Using Blockchain
Published In IJCRT (www.ijcrt.org) & 7.97 Impact Factor by Google Scholar
Volume 12 Issue 9 September 2024 , Date of Publication: 27-September-2024
UGC Approved Journal No: 49023 (18)
PAPER ID : IJCRT2409643
Registration ID : 269802
EDITOR IN CHIEF
Scholarly open access journals, Peer-reviewed, and Refereed Journals, Impact factor 7.97 (Calculate by google scholar and Semantic Scholar | AI-Powered Research Tool) , Multidisciplinary, Monthly Journal
INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS | IJCRT
An International Scholarly, Open Access, Multi-disciplinary, Indexed Journal
Website: www.ijcrt.org | Email id: editor@ijcrt.org | ESTD: 2013
IJCRT | ISSN: 2320-2882 | IJCRT.ORG


Certificate of Publication
INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS | ISSN: 2320 - 2882
An International Open Access, Peer-reviewed, Refereed Journal
The Board of
International Journal of Creative Research Thoughts
Is hereby awarding this certificate to
Pandey Nidhi Mataprasad
In recognition of the publication of the paper entitled
Document Verification And Management System Using Blockchain
Published In IJCRT (www.ijcrt.org) & 7.97 Impact Factor by Google Scholar
Volume 12 Issue 9 September 2024 , Date of Publication: 27-September-2024
UGC Approved Journal No: 49023 (18)
PAPER ID : IJCRT2409643
Registration ID : 269802
EDITOR IN CHIEF
Scholarly open access journals, Peer-reviewed, and Refereed Journals, Impact factor 7.97 (Calculate by google scholar and Semantic Scholar | AI-Powered Research Tool) , Multidisciplinary, Monthly Journal
INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS | IJCRT
An International Scholarly, Open Access, Multi-disciplinary, Indexed Journal
Website: www.ijcrt.org | Email id: editor@ijcrt.org | ESTD: 2013
IJCRT | ISSN: 2320-2882 | IJCRT.ORG

Review Paper:

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Document Verification And Management System Using Blockchain

Gaytri Kumari[1], Prajwalita Dongre[2], Tiya Mukherjee[3], Pandey Nidhi Mataprasad[4]
[1,3,4]UG Student, [2]Professor
[1,2,3,4]Computer Engineering Department,
Sinhgad Academy of Engineering, Pune, Maharashtra, India

Abstract: Documents and certificates are crucial for proving professional achievements, making them essential for career progression. The current system for issuing and verifying these documents is often slow and labour-intensive. Moreover, paper-based documents are susceptible to forgery, resulting in various educational frauds. This project aims to resolve these issues by leveraging blockchain technology. Blockchain extends beyond cryptocurrencies and has significant applications in various fields, including healthcare, supply chain management, and finance. In education, blockchain can transform the traditional method of issuing and verifying certificates. This project will illustrate how professional certificates can be authenticated using the Ethereum platform and smart contracts. The process includes converting traditional paper certificates into digital formats upon request, applying cryptographic hash functions to generate hash values for the digital certificates, storing the hash values on the blockchain, creating a unique certificate ID and transaction hash value, and utilizing the unique certificate ID and transaction hash value for certificate verification through a unified platform. This approach includes streamlining the certificate issuance, storage and verification process, increasing security by preventing forgery and unauthorized modifications, providing a clear and immutable record of certifications, and facilitating easy access and verification by third parties.

Index Terms **- Blockchain, Document, Storage, Security, Ethereum, Hash Function.**

I. INTRODUCTION

The concept of blockchain technology was first described by research scientists Stuart Haber and W. Scott Stornetta, but it became popular in 2009 when Bitcoin was invented by Satoshi Nakamoto. Blockchain technology is now widespread in the educational sector for many use cases, including issuing and verifying documents (e-transcripts), cost-effective large-scale file storage, automated learning platforms, publishing and copyright protection, and payment via cryptocurrencies. Document verification using blockchain is a project powered by the Ethereum Blockchain, which stores and manages student documents. The management process is end-to-end, encompassing both the issuing of documents and their verification. The platform allows the issuer, typically an institution, to issue documents for an entity, which can then use those documents stored on the network to view and verify for authentication and information verification. Blockchain is a distributed ledger and public system that allows for safe and transparent transaction capturing and affirmation. Its distinguishing characteristics, such as irreversibility, transparency, and decentralization, make it an ideal platform for online document verification. By using blockchain, it is possible to establish an encrypted and tamper-proof record of documents, ensuring their integrity and authenticity. This approach provides a more effective and cost-efficient solution while also enhancing security and reducing the likelihood of fraud and errors by blocking fraudulent IDs. In addition to verification, the system offers the feature of storing and retrieving documents using the Inter Planetary File System (IPFS). The documents are stored on IPFS, with their hash values stored on the blockchain, and the backend coding is implemented using smart contracts.

www.ijcrt.org © 2024 IJCRT | Volume 12, Issue 9 September 2024 | ISSN: 2320-2882

II. Literature Review

In "Blockchain Based Verification of Educational and Professional Certificates", The proposed system uses Blockchain technology through the use of public Blockchain and smart contract along with a distributed peer to peer storage called IPFS to store the documents. Published by Anjali Singh, SPS Chauhan, Amit Kumar Goel Professor, School of Computing Science and Engineering, Galgotias University Greater Noida, India.

MIT(Massachusetts Institute of Technology) has achieved issuance and verification of certificates through an application known as Blockcerts using the Bitcoin blockchain. Hashes are generated for every batch of certificates and then they are issued in the blockchain. The website then allows the certificates to be printed using JSON objects.

In "Block Chain Based Document Management System" published in 2001, create an API that is much easier to use and share documents. The system can handle all of the necessary steps for setting up Hyperledger, while also allowing users to write simple API calls for requesting documents, creating documents, adding entries to documents, and giving consent to use a specific type of document. Users will be able to utilize a simpler UI on a website to access the same type of API that allows them to simply create new documents and manage UAC (User Access Control).

"A Blockchain Based Authentication System for Digital Documents" has focused on document verification, while document verification is an important aspect of document management, it is not the only consideration when it comes to managing complex document workflows. Document management systems that only focus on document verification may not be sufficient for organizations that require more granular control over document workflows. By exploring document management systems that offer more advanced workflow management capabilities, organizations can ensure that their document management processes are efficient, secure, and tailored to their specific needs.

The authors from University of Jordan have proposed a system called SmartCert that will be used to issue the certificates as well as verify them using smart contracts. There are two parts of this system, User who can use the national ID to view the certificates and Owner of the contract can create a new certificate. The system works in the following way- If the national ID is invalid then the expected output would be student not found. If the student national ID is valid then the certificate ID number and other details would be the output.

III. Methodology

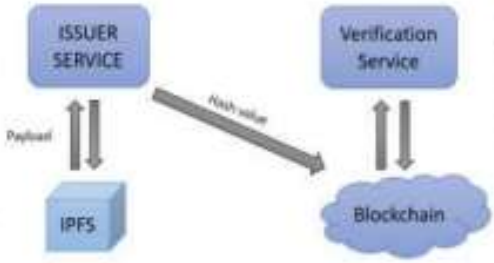

Figure 1: Project Block Diagram

This is a project that aims to implement an efficient anti-forgery mechanism for documents, such as mark sheets, transcripts, diplomas, official identification certificates and other certificates. The goal is to ensure the authenticity of documents, reducing the incidence of counterfeit them, and saving time and financial resources for all parties involved in document verification.

The solution proposed by the project revolves around three roles or entities: **An Issuer, a Verifier, and a User**.

- The issuer is the authority that creates and issues the electronic version of the certificate or document
- Verifier is the potential employer or any person who wants to verify the authenticity of the certificate provided by the user.
- Finally, the user is the recipient of the certificate and can only view the documents issued to him/her.

This is a project that provides an efficient anti-forgery mechanism for documents. By using a combination of blockchain, IPFS, and hash functions, the authenticity of the certificate can be ensured, reducing the incidence of counterfeit certificates and saving time and financial resources for all parties involved in document verification.

www.ijcrt.org © 2024 IJCRT | Volume 12, Issue 9 September 2024 | ISSN: 2320-2882

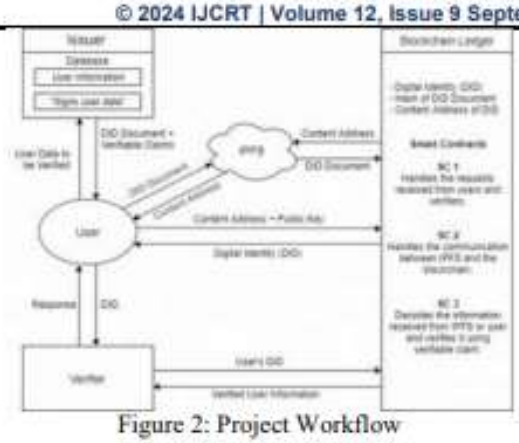

Figure 2: Project Workflow

1. User Registration:
   - User: The user provides his data to the Issuer.
   - Issuer: The issuer captures his data and forms a DID on the database.
   - DID Document: The issuer creates a DID document having the user's data, verifiable claims, and a Content Address.
   - IPFS: This DID document then gets stored on a decentralized data storage network called Inter Planetary File System.

2. Verification Request:
   - Authentication of Claim: The authenticating party sends an authentication request to validate the identity of the user.
   - Recovery of DID Document: The authenticating party retrieves the DID document of the user via its content address using IPFS.

3. Communication with Smart Contract:
   - Smart Contract 1:It is a smart contract that the authenticating party communicates with on the blockchain.
   - Handle Request: Smart Contract 1 receives the authentication request and retrieves the desired information from the DID document.

4. Interaction with IPFS:
   - Smart Contract 2: Smart Contract 2 makes a query to IPFS to retrieve the DID document by its content address.
   - Data Retrieval: The DID document is retrieved from the IPFS, and it sends back to Smart Contract 2.

5. Verification Process:
   - Smart Contract 3: Smart Contract 3 decodes the DID document information and verifies that through verifiable claims.
   - Verification Result: When verification is successful, Smart Contract 3 responds positively to the verifier.

6. Reply to Verifier:
   - Smart Contract 1: Smart Contract 1 returns the outcome of verification back to the verifier.

7. Authentic User Information:
   - Verifier: The verifier gets the outcome of verification and if all good then retrieves the authentic user information.

www.ijcrt.org © 2024 IJCRT | Volume 12, Issue 9 September 2024 | ISSN: 2320-2882

IV. Comparison And Analysis

Feature	Traditional System	Digital System	Blockchain based System
Storage	Physical storage (e.g., filing cabinets)	Cloud-based storage	Decentralized storage on blockchain and IPFS
Accessibility	Limited to physical location	Accessible from anywhere with internet	Accessible from anywhere with internet
Security	Susceptible to physical damage, theft, and unauthorized access	Less susceptible to physical threats but vulnerable to cyberattacks	Highly secure due to immutability of blockchain and distributed nature of IPFS
Tamper-Proofing	Can be altered or forged	Can be altered or forged, but changes can be detected	Tamper-proof due to the cryptographic nature of blockchain and IPFS
transparency	Limited transparency	Increased transparency through audit trails	High transparency due to public nature of blockchain
Efficiency	Manual processes, time-consuming	Highly efficient due to automation and distributed nature	Highly efficient due to automation and distributed nature

Table 1: Traditional System V/S Digital System V/S Blockchain Based System

V. Discussion

Key features: -

- Immutability: After the documents have been recorded on the blockchain, they cannot be modified, ensuring integrity in data.
- Decentralization: No singular authority has control over the system, thereby reducing the risk of potential tampering or loss of data.
- Transparency: All the actions on the blockchain can be traced, therefore providing verifiable audit trails.
- Security: Cryptographic techniques are applied for securing the documents so that any unauthorized access or forgery of them can become almost improbable.
- Authentication: Third-party instant document authentication via any third party without a central authority.
- Smart Contracts: Automate the workflow and process, such as approvals, based on rules established beforehand.
- Access Control: Access is role-based. Hence, only access for which people are authorized can view or modify the documents.
- Cost and Time Efficiency: It reduces paperwork and manual verification. It accelerates the process and saves cost.

Assumptions: -

- The blockchain platform i.e. Ethereum is stable and scalable to handle the expected workload
- Users will be willing to adopt the new system.
- The system can handle various document formats (PDF, Word, Excel, etc.) and metadata.

Dependencies: -

- The development of smart contracts to govern document creation, modification, and access.
- Sufficient storage capacity to accommodate document data on the blockchain.

www.ijcrt.org © 2024 IJCRT | Volume 12, Issue 9 September 2024 | ISSN: 2320-2882

VI. Conclusion

This paper has solved main shortcomings in the existing method of certificate issuance, verification and storage by the concerned parties. The proposed system provides the features of immutability, decentralization and tamper-proof documents which can be verified directly without the need of a third party. Firstly, the scam of fraud certificates since in Blockchain it is easy to trace back the transactions, secondly, this method is faster as compared to the existing method involving paper certificates and finally providing the distributed storage of document using IPFS. The Blockchain technology allows the generation of e-certificates with unique hash values which are then further used to verify the certificates. The unique hash values corresponding to each certificate makes this system more secure and forgery proof.

VII. Acknowledgment

We would like to extend our gratitude to Project staff at the Sinhgad Academy of Engineering, Department of Computer Engineering for their immense support and help without which this work could not have been accomplished. Additionally, we would like to give Mrs. Prajwalita Dongre, our project manager, our profound gratitude for guiding us through the process.

References

[1] Anjali Singh, SPS Chauhan, Amit Kumar Goel Professor, School of Computing Science and Engineering, Galgotias University Greater Noida, India, "Blockchain Based Verification of Educational and Professional Certificates",2023, DOI: 10.1109/ICCSC56913.2023.10143008

[2] SHINYA HAGA AND KAZUMASA OMOTE Faculty of Engineering, Information and Systems, University of Tsukuba, Tsukuba 305-8577, Japan, "Blockchain-Based Autonomous Notarization System Using National eID Card " ,2022, DOI 10.1109/ACCESS.2022.3199744

[3] Mr. S. CHOUDAIAH, Mr. U. CHANDRASELHAR, Dept of MCA, SVEC - Sree Vidyanikethan Engineering College, Tirupati, "Block Chain Based Document Management System", Vol 12, Issue 08, August/2021 ISSN NO:0377-9254

[4] Yerramsetti Sri Uday Kiran Sai Mahesh, Velagapudi Rohith, Vennam Srinivas Reddy , Mrs B. Ratnamala, Dr. Reddyvaari Venkateswara Reddy, "A review on Student Document Management System based on Ethereum Blockchain (PERSONAL- D)", ISSN: 2278-0181 Vol. 12 Issue 08, August-2023

[5] Prof. Renuka Vaidya, Ms. Sanskriti Punde, Mr. Kartikey Yadav, Mr. Chakradhar Ghute, Ms. Namrata Shinde Assistant Professor, Department of Information Technology Students, Department of Information Technology Sinhgad College of Engineering, Pune, India, "Document Management System using Blockchain", Volume 3, Issue 13, May 2023, DOI: 10.48175/568

[6] Moumita Das, Jack C. P. Cheng, Xingyu Tao, "A Secure and Distributed Construction Document Management System Using Blockchain", January 2021 DOI: 10.1007/978-3-030-51295-8_59

[7] Sakshi Jha, Govind Dhingra, Gagan Mittal, Harsh Vardan, Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India "Secured Document Storing Using Blockchain", 2022 IJRTI, Volume 7, Issue 5, ISSN: 2456-3315

Implementation Paper Certificate:

IRJMETS

International Research Journal Of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

e-ISSN: 2582-5208

Ref: IRJMETS/Certificate/Volume 07/Issue 04/70400106561

Date: 13/04/2025

Certificate of Publication

This is to certify that author "**Gaytri Kumari**" with paper ID "**IRJMETS70400106561**" has published a paper entitled "DOCUMENT VERIFICATION AND MANAGEMENT SYSTEM USING BLOCKCHAIN" **in International Research Journal Of Modernization In Engineering Technology And Science (IRJMETS), Volume 07, Issue 04, April 2025**

Editor in Chief

IRJMETS Impact Factor 8.187

We Wish For Your Better Future

www.irjmets.com

Google Scholar ISSUU Academia.edu doi Crossref Content Registration

IRJMETS

International Research Journal Of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

e-ISSN: 2582-5208

Ref: IRJMETS/Certificate/Volume 07/Issue 04/70400106561

Date: 13/04/2025

Certificate of Publication

This is to certify that author "**Prajwalita Dongre**" with paper ID "**IRJMETS70400106561**" has published a paper entitled "DOCUMENT VERIFICATION AND MANAGEMENT SYSTEM USING BLOCKCHAIN" **in International Research Journal Of Modernization In Engineering Technology And Science (IRJMETS), Volume 07, Issue 04, April 2025**

Editor in Chief

IRJMETS Impact Factor 8.187

We Wish For Your Better Future

www.irjmets.com

Google scholar ISSUU Academia.edu doi Crossref Content Registration

International Research Journal Of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

e-ISSN: 2582-5208

Ref: IRJMETS/Certificate/Volume 07/Issue 04/70400106561

Date: 13/04/2025

Certificate of Publication

This is to certify that author "**Tiya Mukherjee**" with paper ID "**IRJMETS70400106561**" has published a paper entitled "DOCUMENT VERIFICATION AND MANAGEMENT SYSTEM USING BLOCKCHAIN" **in International Research Journal Of Modernization In Engineering Technology And Science (IRJMETS), Volume 07, Issue 04, April 2025**

Editor in Chief

IRJMETS Impact Factor 8.187

We Wish For Your Better Future

www.irjmets.com

IRJMETS

International Research Journal Of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

e-ISSN: 2582-5208

Ref: IRJMETS/Certificate/Volume 07/Issue 04/70400106561

Date: 13/04/2025

Certificate of Publication

This is to certify that author "**Tiya Mukherjee**" with paper ID "**IRJMETS70400106561**" has published a paper entitled "DOCUMENT VERIFICATION AND MANAGEMENT SYSTEM USING BLOCKCHAIN" **in International Research Journal Of Modernization In Engineering Technology And Science (IRJMETS), Volume 07, Issue 04, April 2025**

Editor in Chief

IRJMETS Impact Factor 8.187

We Wish For Your Better Future

www.irjmets.com

Google scholar ISSUU Academia.edu doi Crossref Content Registration

Implementation Paper:

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

DOCUMENT VERIFICATION AND MANAGEMENT SYSTEM USING BLOCKCHAIN

Gaytri Kumari*1, Prajwalita Dongre*2, Tiya Mukherjee*3, Pandey Nidhi Mataprasad*4
*1,2,3,4Computer Department, Sinhgad Academy Of Engineering, Pune, Maharashtra, India.

ABSTRACT

Documents and certificates are of primary importance when establishing professional achievements and are thus key to career development. The present mechanism of issuance and authentication of these documents tends to be cumbersome and time-consuming. Further, paper documents can be forged easily, leading to numerous education-related frauds. This project focuses on solving the above issues using blockchain technology. Blockchain goes beyond cryptocurrencies and has a wide range of applications in other areas, such as healthcare, supply chain management, and finance. In education, blockchain can revolutionize the conventional way of issuing and validating certificates. This project will demonstrate how professional certificates can be verified using the Ethereum platform and smart contracts. The process involves converting paper certificates into digital form on demand, using cryptographic hash functions to produce hash values for the digital certificates, storing the hash values on the blockchain, generating a unique certificate ID and transaction hash value, and using the unique certificate ID and transaction hash value for certificate verification through a common platform. It covers streamlining certificate issuance, storage, and verification, enhancing security to prevent forging and unauthorized amendment, ensuring clear and unchangeable record of certification, as well as simplifying third-party easy access and verification.

Keywords: Blockchain, Document, Storage, Security, Ethereum, Hash Function.

I. INTRODUCTION

The idea of blockchain technology was originally explained by research scientists Stuart Haber and W. Scott Stornetta, but it came to prominence in 2009 with the invention of Bitcoin by Satoshi Nakamoto. Blockchain technology has spread extensively in the educational field for numerous applications, such as issuance and authentication of documents (e-transcripts), inexpensive storage of large files, automated learning platforms, publishing and protection of copyright, and payment in the form of cryptocurrencies. Document verification with blockchain is an initiative fueled by the Ethereum Blockchain, where student documents are stored and maintained. Management is end-to-end, covering both issuing documents and verifying them. The issuer, in most cases an institution, has the authority to issue documents for an entity, and then entities can utilize the stored documents on the network to view and verify to check for authenticity and verification of information. Blockchain is a distributed ledger and public network that enables secure and transparent capturing and confirmation of transactions. Its unique features, including irreversibility, transparency, and decentralization, are well-suited for online document authentication. Through blockchain, it is conceivable to create an encrypted and tamper-proof document record, which guarantees their integrity and authenticity. Such an approach is better, cost-friendly, and both enhances security, decreases chances of fraud and error, and is done by rejecting fraudulent IDs. Apart from the verification aspect, the system possesses the capability for storing and recovering documents with the use of Inter Planetary File System (IPFS). Such documents are on IPFS stored while their hash values are retained on the blockchain, and back-end coding takes place using the use of smart contracts.

II. LITERATURE SURVEY

Blockchain technology has emerged as a robust solution for verifying educational and professional certificates, addressing the longstanding issues of document forgery, inefficiency, and lack of transparency. Traditional methods, which often involve manual verification by third-party entities, are prone to delays and fraud. For instance, paper-based certificates can be easily damaged, lost, or tampered with, leading to challenges in authenticating a candidate's credentials. In educational contexts, institutions can digitally issue certificates, hash them using cryptographic functions, and store these hashes on a blockchain. This method, utilized by projects like the one proposed by Anjali Singh et al., ensures that any attempt to alter the certificate would

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

result in a hash mismatch, making the forgery detectable. The Ethereum blockchain, combined with smart contracts, plays a critical role in automating the verification process. Once a certificate is uploaded and hashed, it is stored on the blockchain alongside a unique transaction ID, which can be referenced for future validation [1].

By leveraging blockchain, these problems can be mitigated through its immutable, decentralized, and transparent nature. In related research, the use of a national eID card for notarization further exemplifies blockchain's capability in secure document verification. This approach integrates Public Key Infrastructure (PKI) to authenticate the issuer's identity, effectively replacing traditional notary services with automated smart contracts [2].

Blockchain-based DMS also promotes data ownership and transparency, as users control their records and can grant or revoke access as needed. In both SDMS and CDMS, decentralized networks eliminate reliance on a single authority, significantly reducing risks associated with data breaches and unauthorized access. The technology also helps prevent fraud through non-repudiable transaction records, reducing disputes and improving accountability. These blockchain-based solutions, therefore, revolutionize document management by reinforcing security, ensuring transparency, and providing participants with direct control over their data, paving the way for more efficient, scalable, and trust-based digital ecosystems [3].

Document Management System (SDMS) based on Ethereum, blockchain technology safeguards student records by enabling immutable and decentralized storage, which facilitates the prevention of unauthorized document modifications. Smart contracts on the Ethereum blockchain automate verification processes, streamlining operations, and minimizing administrative workload, making the process more reliable and error-free [4].

Additionally, systems like the one developed by Prof. Renuka Vaidya and team focus on document management by combining blockchain with IPFS (Inter Planetary File System), enabling secure, decentralized storage and easy retrieval of documents [5].

Additionally, construction-specific DMS (CDMS) frameworks utilize blockchain and Interplanetary File System (IPFS) storage for managing extensive and complex project documentation, enhancing security by distributing control across participants. In this system, a cryptographic indexing structure and smart contracts are used to establish secure workflows, track document versions, and uphold data consistency, providing a structured yet flexible solution for the unique demands of construction projects [6].

Blockchain-based Decentralized Personal Document Locker, which addresses the need for secure storage without centralized control. It proposes using blockchain to maintain the immutability and integrity of documents. Another work, Distributed Data Sharing System based on Smart contract and IPFS, examines the benefits of using blockchain combined with decentralized storage like IPFS to enhance data security and accessibility. Additionally, other research highlights the role of cryptographic methods like symmetric and asymmetric encryption in ensuring data privacy, confidentiality, and authenticity [7].

III. METHODOLOGY

This is a project that seeks to deploy an effective anti-forgery mechanism for documents, including mark sheets, transcripts, diplomas, official identification certificates and other certificates. The intention is to provide assurance of the authenticity of documents, minimizing the occurrence of forging them, and conserving time and financial resources for all parties involved in document verification.

The project's solution is based on three roles or parties: An Issuer, a Verifier, and a User.

- The issuer is the entity that generates and issues the electronic certificate or document
- Verifier is the prospective employer or any individual who wishes to check the authenticity of the certificate presented by the user.
- Lastly, the user is the one receiving the certificate and can only see the documents issued to him/her.

This is a project that offers an effective anti-forgery solution for documents. With the application of a combination of blockchain, IPFS, and hash functions, the authenticity of the certificate can be guaranteed, minimizing the occurrence of fake certificates and saving time and financial resources for all parties involved in document verification.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

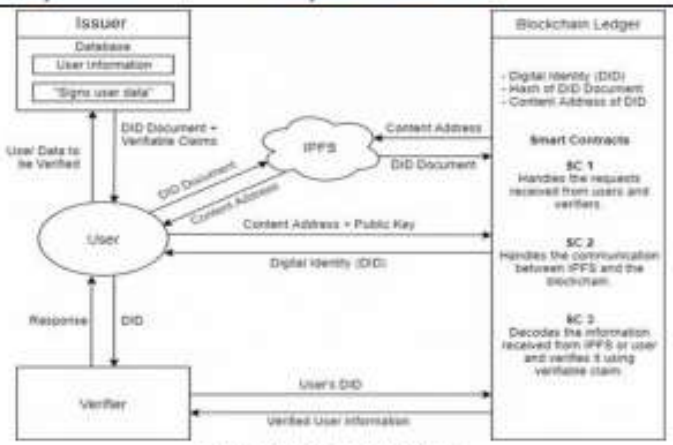

Figure 1: Project Workflow

IV. MODELING AND ANALYSIS

Analysis

Below is a comprehensive list of functional requirements that the system seeks to fulfill:

a. System enables users to link to MetaMask wallets.
b. System enables the issuer to issue certificates to users.
c. System gives IPFS links on issuing documents.
d. System enables users to see a list of issued certificates.
e. System provides verification results on submitting details of documents by verifier.

The following is a comprehensive list of non-functional requirements that the system is seeking to fulfill:

a. Usability: The system is designed on generic UX principles thus ensuring a seamless user experience
b. Reliability and Availability: In the event of any bugs, proper error-handling mechanism will be used so there is always some minimal functionality present
c. Capacity: As the project deals with blockchain, a considerate amount of memory is required and high computation at server side
d. Maintainability: Code will be designed following SOLID principles for designing minimum technical debt
e. Security: Blockchain as immutable ledger will introduce an additional level of security

Design Details

Following Ideal Software Development Design Principles will be observed while designing the application

Don't repeat yourself (DRY): The DRY principle is expressed as "Every piece of knowledge must have a single, unambiguous, authoritative representation within a system". The principle has been developed by Andy Hunt and Dave Thomas in their book The Pragmatic Programmer. They use it rather generally to encompass "database schemas, test plans, the build system, even documentation". When the DRY principle is implemented successfully, a change of any one element of a system does not necessitate a change in other logically unrelated elements.

You aren't gonna need it (YAGNI): Always implement things when you really need them, never when you simply anticipate that you need them

Solid principles: Robert C. Martin came up with SOLID principle which is also called Uncle Bob and it is programming coding standard. This principle is an acronym of the five principles which is given below.

- Single Responsibility Principle (SRP)
- Open/Closed Principle
- Liskov's Substitution Principle (LSP)
- Interface Segregation Principle (ISP)
- Dependency Inversion Principle (DIP)

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

Architecture diagram

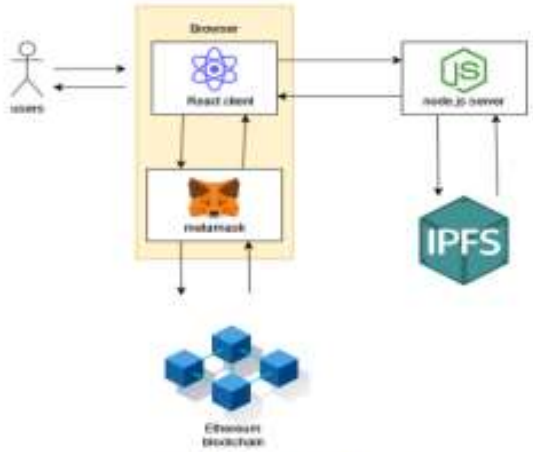

Figure 2: System Architecture

V. RESULTS AND DISCUSSION

Implementation result

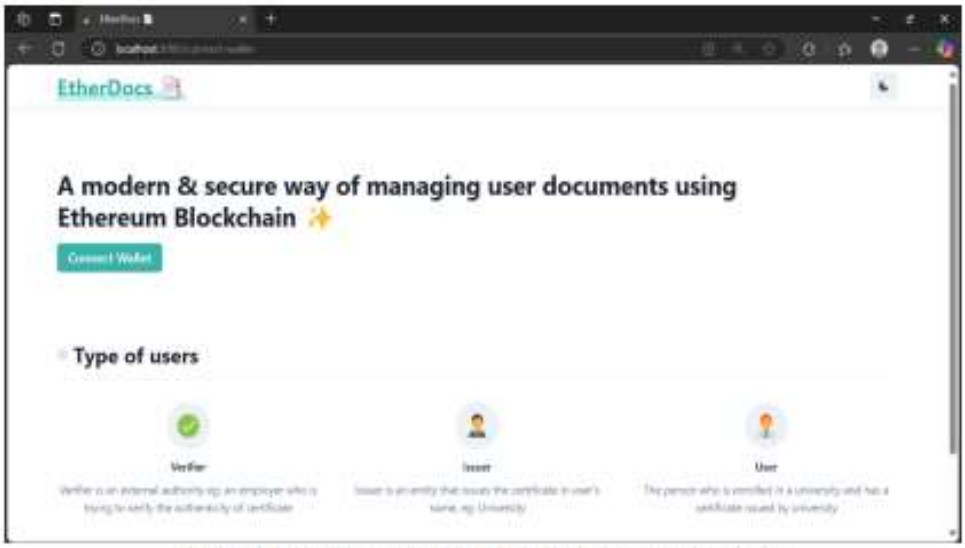

Figure 3: Homepage describing the 3 roles: Issuer, Verifier & User

As shown in Fig. The system revolves around three key roles or entities: the issuer, the verifier, and the user. The issuer, typically a university or other academic institution, creates an electronic version of the certificate to be issued, along with a unique UUID printed on the document, and a hash value of the document. The certificate is uploaded to the InterPlanetary File System (IPFS), and all data related to the certificate and IPFS link along with the hash value of document is stored on the blockchain. The verifier, typically a potential employer or other interested party, can verify the authenticity of the document by comparing the hash value of the document with the hash value stored on the blockchain. The student can only view the documents issued to them.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

Figure 4: Choosing the role

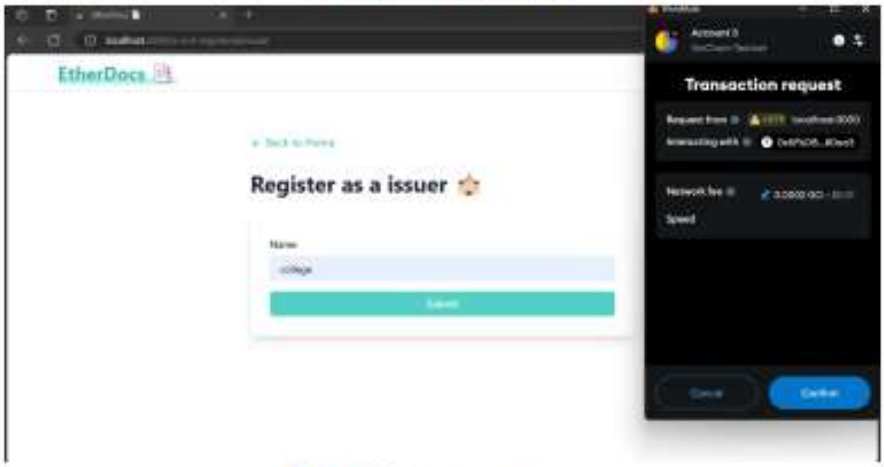

Figure 5: Registering new issuer

The process starts with the issuer creating an electronic version of the certificate to be issued. The electronic version of the certificate contains a hash value of the document, a unique UUID printed on the document. The hash value of the document is a unique digital fingerprint that is generated using a hash function. The UUID is a unique identifier that is assigned to the certificate, and the IPFS link is used to access the certificate on IPFS, a distributed file system.

Once the certificate is created, it is uploaded to IPFS, where it can be accessed by the user. All the data related to the certificate and the IPFS link are stored on the blockchain. The blockchain is a distributed ledger that is tamper-proof and immutable, making it an ideal platform for storing data that needs to be secured.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

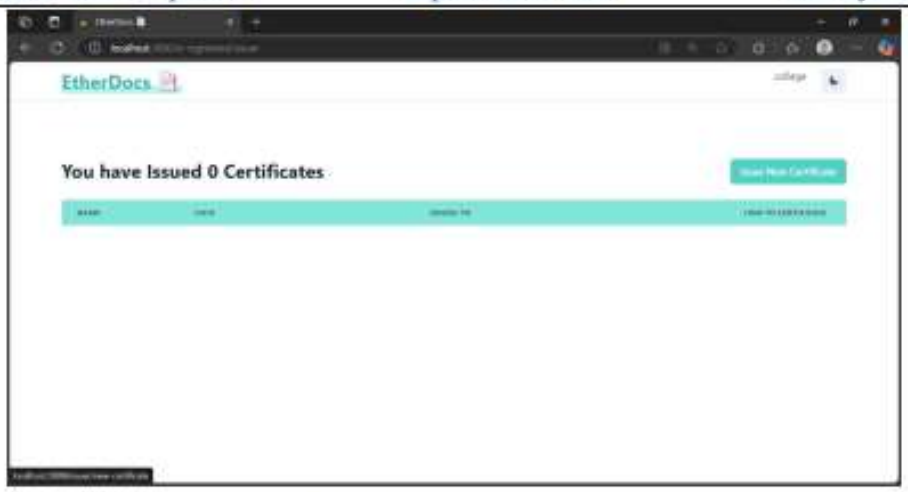

Figure 6: Home Page of issuer

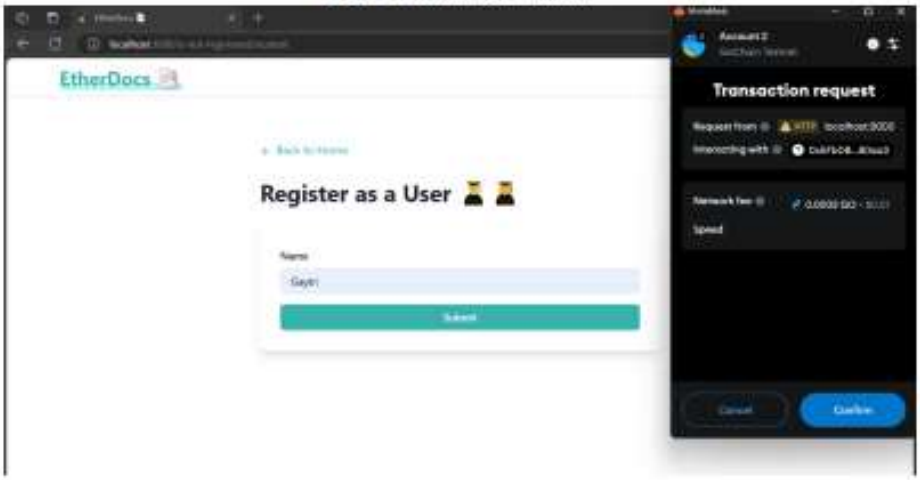

Figure 7: registering new user

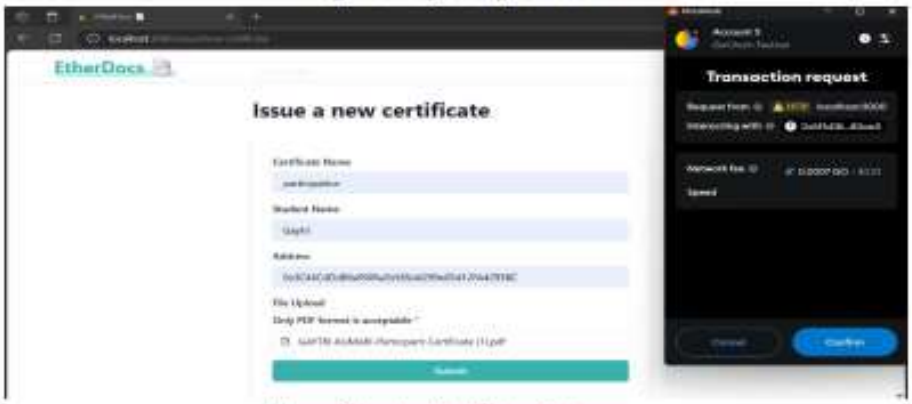

Figure 8: Issuing Certificate for the user

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

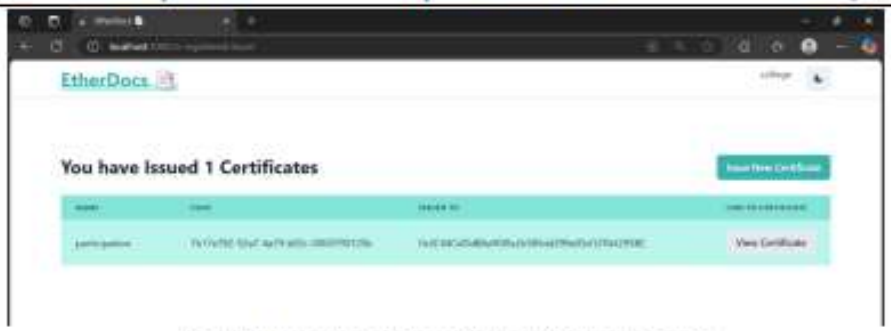

Figure 9: Home Page of issuer After certificate was issued

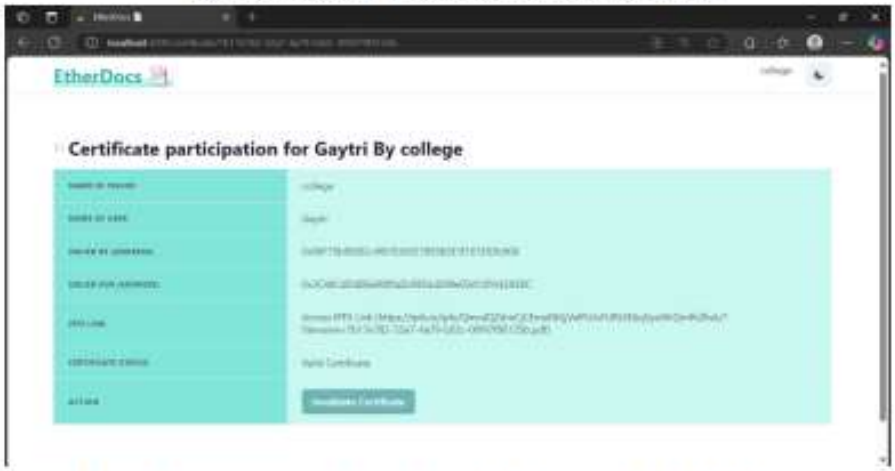

Figure 10: Certificate detail page of issuer with feature to Invalidate Certificate

Figure 11: Issued Ceritificate on IPFS with UUID

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

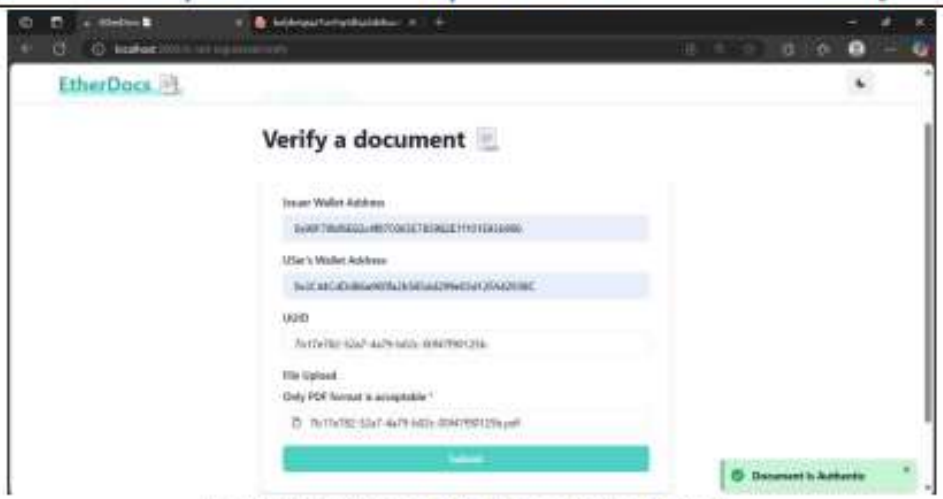

Figure 12: Verification of Certificate at the Verifier's end

In summary, the solution, This a project that provides an efficient anti-forgery mechanism for academic documents. By using a combination of blockchain, IPFS, and hash functions, the authenticity of the certificate can be ensured, reducing the incidence of counterfeit certificates and saving time and financial resources for all parties involved in document verification. This proposed solution has been implemented successfully.

VI. CONCLUSION

This paper has addressed primary deficiencies in the current method of certificate issuance, verification and storage by the respective parties. The suggested system offers the aspects of immutability, decentralization and tamper-proof documents which can be verified directly without involving a third party. Firstly, the fraud certificate scam because in Blockchain it is simple to trace back the transactions, secondly the process is quicker compared to the current method using paper certificates and lastly offering the distributed storage of the document using IPFS. The Blockchain technology facilitates the creation of e-certificates with special hash values which are further utilized to validate the certificates. The use of unique hash values corresponding to each certificate renders this system more secure and forgery proof.

ACKNOWLEDGEMENTS

We would like to extend our gratitude to Project staff at the Sinhgad Academy of Engineering, Department of Computer Engineering for their immense support and help without which this work could not have been accomplished. Additionally, we would like to give Mrs. Prajwalita Dongre, our project manager, our profound gratitude for guiding us through the process.

VII. REFERENCES

[1] Anjali Singh, SPS Chauhan, Amit Kumar Goel Professor, School of Computing Science and Engineering, Galgotias University Greater Noida, India, "Blockchain Based Verification of Educational and Professional Certificates",2023, DOI: 10.1109/ICCSC56913.2023.10143008

[2] SHINYA HAGA AND KAZUMASA OMOTE Faculty of Engineering, Information and Systems, University of Tsukuba, Tsukuba 305-8577, Japan, "Blockchain-Based Autonomous Notarization System Using National eID Card " ,2022, DOI 10.1109/ACCESS.2022.3199744

[3] Mr. S. CHOUDAIAH, Mr. U. CHANDRASELHAR, Dept of MCA, SVEC - Sree Vidyanikethan Engineering College, Tirupati, "Block Chain Based Document Management System", Vol 12, Issue 08, August/2021 ISSN NO:0377-9254

[4] Yerramsetti Sri Uday Kiran Sai Mahesh, Velagapudi Rohith, Vennam Srinivas Reddy , Mrs B. Ratnamala, Dr. Reddyvaari Venkateswara Reddy, "A review on Student Document Management System based on Ethereum Blockchain (PERSONAL- D)", ISSN: 2278-0181 Vol. 12 Issue 08, August-2023

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:04/April-2025 Impact Factor- 8.187 www.irjmets.com

[5] Prof. Renuka Vaidya, Ms. Sanskriti Punde, Mr. Kartikey Yadav, Mr. Chakradhar Ghute, Ms. Namrata Shinde Assistant Professor, Department of Information Technology Students, Department of Information Technology Sinhgad College of Engineering, Pune, India, "Document Management System using Blockchain", Volume 3, Issue 13, May 2023, DOI: 10.48175/568

[6] Moumita Das, Jack C. P. Cheng, Xingyu Tao, "A Secure and Distributed Construction Document Management System Using Blockchain", January 2021 DOI: 10.1007/978-3-030-51295-8_59

[7] Sakshi Jha, Govind Dhingra, Gagan Mittal, Harsh Vardan, Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India ,"Secured Document Storing Using Blockchain", 2022 IJRTI, Volume 7, Issue 5, ISSN: 2456-3315

[8] Qurotul Aini, Eka Purnama Harahap, Nuke Puji Lestari Santoso, Siti Nurindah Sari, Po Abas Sunarya, University of Raharja, Tangerang, Indonesia," Blockchain Based Certificate Verification System Management", Vol. 7, No. 3, 2023, pp. 1~10,E-ISSN: 2622-6804 P-ISSN: 2622-6812, DOI: 10.34306

[9] Isyak Meirobiea, Agustinus Purna Irawanb, Husni Teja Sukmanac, Diana Putri Lazirkhad, Nuke Puji Lestari Santoso, Tarumanagara University, Letjen S. Parman Street No. 1, Jakarta 11440, Indonesia," Framework Authentication e-document using Blockchain Technology on the Government system", International Journal of Artificial Intelegence Research ISSN: 2579-7298,Vol 6, No 2, December 2022

[10] Xue Zhai, Shanchen Pang, Min Wang ,Sibo Qiao ,Zhihan Lv," TVS: a trusted verification scheme for office documents based on blockchain", Complex & Intelligent Systems, https://doi.org/10.1007/s40747-021-00617-1, 3 December 2021

APPENDIX B

Plagiarism Report: