**DOQFY- DOCUMENT VERIFICATION USING**

**BLOCKCHAIN**

## A PROJECT REPORT

***Submitted by***

|  |  |
| --- | --- |
| **G. KAVIYABHARATHI** | **812420104041** |
| **S. MOHAMED TAWFEEQ** | **812420104060** |
| **K. MOHAMED YUNUS** | **812420104062** |
| **M. MUFTHI MOHAMED** | **812420104064** |

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

***degree of***

# BACHELOR OF ENGINEERING

***in***

**COMPUTER SCIENCE AND ENGINEERING**

**M.I.E.T. ENGINEERING COLLEGE, TRICHY– 620 007**

# ANNA UNIVERSITY :: CHENNAI – 600 025



## MAY 2024

**ANNA UNIVERSITY : CHENNAI 600 025**

# BONAFIDE CERTIFICATE

Certified that this project report “**DOQFY – DOCUMENT VERIFICATION USING BLOCKCHAIN”** is the Bonafide of **“G.KAVIYABHARATHI” (812420104041), “S.MOHAMED TAWFEEQ” (812420104060), “K.MOHAMED YUNUS” (812420104062), “M.MUFTHI MOHAMED” (812420104064)** who carried out the

project under the supervision.

## SIGNATURE SIGNATURE

Mr.P.MANIKANDAN M.E., Mrs.R.DEEPA M.E.,

## HEAD OF THE DEPARTMENT SUPERVISOR ASSISTANT PROFESSOR

Department of Computer Science and Department of Computer Science and Engineering Engineering

M.I.E.T. Engineering College, M.I.E.T. Engineering College,

Trichy – 620 007 Trichy – 620 007

Submitted for the viva-voce held on

**INTERNAL EXAMINER EXTERNAL EXAMINER**

# ACKNOWLEDGMENT

First of all we thank God for this shower of blessing and his divine help which enables us to complete the project successfully.

We extend our sincere thanks to **Alhaj.Janab.Er.A.MOHAMED YUNUS, B.E., M.Sc., (Engg.)** Founder & Chairman of M.I.E.T Engineering College, Trichy for offering the means of attaining our most cherished Goal Environment.

We extend our deepest gratitude to Principal **Dr.A.NAVEEN SAIT,M.E, Ph.D.** M.I.E.T. Engineering College, Trichy, for giving us permission to do the project work successfully.

We are grateful to express our profound thanks to head of the department, **Mr.P.MANIKANDAN,M.E.,** Assistant Professor who has been the source of encouragement and moral strength throughout our study period

It gives immense pleasure to extend my sincere and heartfelt gratitude to our project Guide **Mrs.R.DEEPA M.E,** Assistant Professor for her untiring valuable and timely suggestions in dispensable situation during the period of study.

We are extremely thankful to our parents for enlightening us by providing Professional education and for their prayerful support that makes us to complete.

Also heartfelt thanks to our friends, Teaching and Non-teaching staff members who helped us to finish the project successfully.

# ABSTRACT

Utilization of blockchain technology for document verification, with a specific focus on enhancing digital copyright management. Traditional methods encounter challenges in confirming, authorizing, and maintaining digital rights. Leveraging blockchain's decentralized structure and cryptographic foundations, this study proposes an innovative approach to bolster trust in digital copyright management. By harnessing self-supervision, traceability, and decentralization inherent in blockchain, along with advanced features like the Map function, DoQfy aims to augment data transmission rates and precision in the multi-channel model. Through the implementation of blockchain-based solutions, the likelihood of various digital copyright infringement incidents is significantly mitigated, paving the way for more robust and efficient document verification procedures.

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TABLE OF CONTENTS**  **TITLE** | **PAGE NO.** |
|  | **ABSTRACT** | **iv** |
|  | **LIST OF FIGURES** | **viii** |
| **1.** | **INTRODUCTION** | **1** |
| **2.** | **LITERATURE SURVEY** | **3** |

* 1. SECURE DOCUMENT VERIFICATION 3

USING BLOCKCHAIN AND ZERO- KNOWLEDGE PROOFS

* 1. DECENTRALIZED DOCUMENT 5

VERIFICATION USING BLOCKCHAIN

* 1. BLOCKCHAIN TECHNOLOGY FOR 7

DOCUMENT VERIFICATION: A REVIEW

* 1. ENHANCING DIGITAL COPYRIGHT 9

MANAGEMENT WITH BLOCKCHAIN

* 1. BLOCKCHAIN - BASED DOCUMENT 11

VERIFICATION: CHALLENGES AND

OPPURTUNITIES

**3.**

**SYSTEM ANALYSIS**

**11**

11

3.1 EXISTING SYSTEM

|  |  |
| --- | --- |
| 3.1.1 Disadvantages |  |
| 3.2 PROPOSED SYSTEM | 14 |
| 3.2.1 Advantages | 15 |

**4. SYSTEM REQUIREMENTS 16**

4.1 HARDWARE REQUIREMENTS 16

4.2 SOFTWARE REQUIREMENTS 16

5. SYSTEM DESIGN 17

* 1. [SYSTEM ARCHITECTURE 17](#_TOC_250004)
  2. [DATAFLOW DIAGRAM 19](#_TOC_250003)
  3. [USE CASE DIAGRAM 21](#_TOC_250002)
  4. [CLASS DIAGRAM 23](#_TOC_250001)

5.5 [SEQUENCE DIAGRAM 24](#_TOC_250000)

6. MODULE DESCRIPTION 26

|  |  |
| --- | --- |
| 6.1 LIST OF MODULES | 26 |
| 6.1.1 Decentralized User Verification Module | 26 |
| 6.1.2 Identity Verification Module | 27 |
| 6.1.3 Student Identity Vault Module | 29 |
| 6.1.4 Credential Forge Module | 32 |
| 6.1.5 Hire Guard Module | 33 |

|  |  |  |
| --- | --- | --- |
| **7.** | **CONCLUSION AND FUTURE**  **ENHANCEMENT** | **36** |

* 1. CONCLUSION 36

7.2 FUTURE ENHANCEMENT 37

**APPENDICES 39**

1. SAMPLE CODE 39
2. SCREENSHOTS 54

**REFERENCES 61**

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **FIGURE NO.** | **FIGURE NAME** | **PAGE NO.** |

|  |  |  |
| --- | --- | --- |
| 5.1 | System Architecture | 17 |
| 5.2 | Dataflow Diagram | 19 |
| 5.3 | Use Case Diagram | 21 |
| 5.4 | Class Diagram | 23 |

24

|  |  |
| --- | --- |
| 5.5 | Sequence Diagram |

54

|  |  |
| --- | --- |
| A.2.1 | Home Page |

55

|  |  |
| --- | --- |
| A.2.2 | Login Page |

56

|  |  |
| --- | --- |
| A.2.3 | University Page |

57

|  |  |
| --- | --- |
| A.2.4 | Student Page |

58

|  |  |
| --- | --- |
| A.2.5 | Company Page |

59

|  |  |
| --- | --- |
| A.2.6 | IPFS Connect |

60

|  |  |
| --- | --- |
| A.2.7 | Transaction Page |

# CHAPTER 1 INTRODUCTION

In an increasingly digitized world where personal data is often centralized and vulnerable to security breaches, the need for a robust and secure identity management system has never been more crucial. A Decentralized Identity Management System represents a paradigm shift in how individuals assert and control their identities in the digital realm.

By leveraging decentralized technologies such as blockchain, this innovative system enables users to register, verify, and manage their identities autonomously, without relying on centralized authorities or intermediaries. Each user retains full ownership and control over their identity data, which is cryptographically secured and tamper-proof, ensuring privacy, security, and user empowerment. Through a combination of cryptographic techniques, peer-to-peer networks, and self-sovereign identity principles, decentralized identity management systems offer a transformative solution to the challenges of identity theft, data breaches, and digital identity fraud

This introduction explores the fundamental concepts, principles, and benefits of decentralized identity management systems, highlighting their potential to revolutionize the way individuals interact, transact, and engage in the digital world.

In addition to enhancing security and privacy, a Decentralized Identity Management System fosters a more inclusive and interoperable digital ecosystem. Traditional identity systems often suffer from fragmentation and lack of interoperability, requiring users to create and manage multiple accounts across various platforms.

In contrast, a decentralized approach enables seamless integration and portability of identities across different services and applications. Users have the flexibility to selectively disclose and share their identity attributes based on specific contexts and consent, promoting trust and reducing friction in digital interactions. Moreover, decentralized identity standards and protocols facilitate cross-platform compatibility and collaboration, enabling developers to build innovative applications and services that leverage decentralized identities. By promoting user-centricity, interoperability, and innovation, decentralized identity management systems lay the foundation for a more equitable, efficient, and secure digital future. Beyond individual empowerment, Decentralized Identity Management Systems hold significant promise for revolutionizing various industries and sectors. From financial services to healthcare, education, and beyond, the ability to securely and verifiably manage digital identities opens up new possibilities for innovation and efficiency. Through this project, we seek to address the limitations of traditional document verification methods and pave the way for a more efficient, transparent, and secure approach to document verification in the digital age.

# CHAPTER 2 LITERATURE SURVEY

## SECURE DOCUMENT VERIFICATION USING BLOCKCHAIN AND ZERO-

**KNOWLEDGE**

**AUTHOR:** Smith, J. et al. (2018)

## DESCRIPTION:

The literature survey on "Secure Document Verification Using Blockchain and Zero-Knowledge" offers an in-depth exploration into the intersection of blockchain technology and zero-knowledge proofs, focusing on their combined potential to revolutionize document verification processes. This comprehensive survey delves into the theoretical underpinnings, practical implementations, and emerging trends in leveraging these cutting-edge technologies for enhancing document security, transparency, and privacy.

The survey begins by providing a thorough examination of blockchain technology, elucidating its fundamental principles, including decentralization, immutability, and consensus mechanisms. It explores how blockchain-based distributed ledgers serve as a secure and transparent repository for storing document records, enabling tamper-proof verification and audit trails. Additionally, the survey delves into the mechanics of zero-knowledge proofs, unpacking their cryptographic intricacies and their role in enabling verification without the need for revealing sensitive information.

Furthermore, the literature survey investigates the convergence of blockchain and zero-knowledge proofs in the context of document verification, analyzing how these technologies complement each other to address key challenges in document security and privacy. It explores various cryptographic protocols, such as zk-SNARKs and zk-STARKs, and their applications in document verification scenarios, including proof of authenticity, ownership, and integrity.

The survey reviews a wide array of research papers, academic studies, and real-world implementations of secure document verification systems leveraging blockchain and zero-knowledge proofs across diverse domains, including finance, healthcare, supply chain management, and government services. It critically evaluates the strengths and limitations of existing systems, identifies emerging trends and challenges, and offers insights into best practices and future research directions.Moreover, the survey discusses the broader implications of adopting blockchain and zero-knowledge-based document verification systems, including their potential impact on data privacy, regulatory compliance, and interoperability. It examines the legal and ethical considerations surrounding the implementation of such systems, highlighting the importance of data protection, user consent, and transparency in ensuring trust and accountability.

In conclusion, the literature survey on "Secure Document Verification Using Blockchain and Zero-Knowledge" serves as an authoritative guide for researchers, practitioners, and policymakers seeking to navigate the complex landscape of document security and privacy in the digital age. With its comprehensive coverage of theoretical concepts, practical implementations, and future prospects, the survey offers valuable insights and perspectives on harnessing blockchain and zero-knowledge proofs to revolutionize document verification processes and enhance trust in digital transactions.

## DECENTRALIZED DOCUMENT VERIFICATION USING BLOCKCHAIN

**AUTHOR:** Patel, A. et al **(**2019) **DESCRIPTION:**

In recent years, there has been growing interest in utilizing blockchain technology for decentralized document verification. Traditional methods of document verification often rely on centralized authorities or intermediaries, which can introduce

inefficiencies, security vulnerabilities, and dependencies on third parties. However, blockchain offers a decentralized and tamper-resistant alternative that can streamline the document verification process while enhancing security and transparency.

Several studies and projects have explored the feasibility and effectiveness of using blockchain for decentralized document verification. These works have highlighted the potential of blockchain to address the limitations of centralized verification systems by providing a secure, transparent, and decentralized infrastructure for verifying documents.

One notable project in this area is the development of decentralized identity platforms based on blockchain technology. These platforms enable individuals to create and manage their digital identities on a blockchain, allowing them to verify their identity and authenticate documents without relying on centralized authorities. By decentralizing identity management, these platforms empower individuals to control their own identity information and streamline the document verification process.

Additionally, research has focused on leveraging smart contracts, self- executing contracts with the terms of the agreement directly written into code, to automate and enforce document verification processes on the blockchain. Smart contracts can

facilitate the issuance, validation, and revocation of documents in a transparent and tamper-proof manner, eliminating the need for intermediaries and reducing the risk of fraud.

Furthermore, blockchain-based document verification systems offer

potential benefits such as increased security, data integrity, and auditability. The immutability of blockchain ensures that once a document is verified and recorded on the blockchain, it cannot be altered or deleted, providing a reliable and tamper-proof record of document authenticity.

Overall, the literature on decentralized document verification using blockchain underscores the transformative potential of this technology in enhancing the security, efficiency, and transparency of document verification processes. By leveraging blockchain's decentralized architecture, immutability, and smart contract capabilities, decentralized document verification systems have the potential to revolutionize the way documents are verified and authenticated in various domains. By leveraging blockchain's decentralized architecture and smart contract capabilities, cross-border document verification processes can be automated and standardized, facilitating smoother and more efficient verification of documents across jurisdictions. This has the potential to benefit various sectors, including international trade, immigration, and global supply chains, by reducing administrative burdens and improving the reliability of document verification.

## BLOCKCHAIN TECHNOLOGY FOR DOCUMENT VERIFICATION: A REVIEW

**AUTHOR:** Garcia, M. et al.

## DESCRIPTION:

Blockchain technology has garnered significant attention for its potential to revolutionize document verification processes across various industries. This literature survey provides a comprehensive review of the research and developments in utilizing blockchain for document verification purposes.The survey begins by examining the fundamental principles of blockchain technology and its relevance to document verification. It explores how blockchain's decentralized and immutable nature can address the shortcomings of traditional verification methods, such as reliance on centralized authorities and susceptibility to tampering.

Furthermore, the survey investigates the potential societal and economic implications of adopting blockchain technology for document verification on a global scale. It explores how blockchain has the potential to democratize access to verification

services, particularly in regions with limited infrastructure or trust in centralized authorities. By providing a decentralized and transparent platform for document verification, blockchain can empower individuals and organizations to assert ownership of their data and credentials, fostering greater autonomy and inclusivity. Moreover, the survey examines the potential economic benefits of blockchain-based verification systems, such as reduced transaction costs, increased efficiency, and enhanced trust among stakeholders. Additionally, it considers the broader implications for industries undergoing digital transformation, including implications for regulatory frameworks, business models, and market dynamics. By exploring the broader societal and economic implications, this survey aims to provide a holistic understanding of the transformative potential of

blockchain.

Moreover, the survey delves into the technical intricacies of blockchain technology and its applicability to document verification. It examines various consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS), and evaluates their suitability for document verification systems in terms of scalability, security, and energy efficiency. Additionally, the survey explores different blockchain architectures, including public, private, and consortium blockchains, and their implications for document verification use cases. Furthermore, it discusses the role of cryptographic techniques, such as hash functions, digital signatures, and Merkle trees, in ensuring data integrity and authentication in blockchain-based verification systems. By providing an in-depth analysis of the technical aspects of blockchain technology, this survey aims to elucidate the underlying mechanisms that enable secure and reliable document verification on blockchain platforms.

Additionally, the survey examines the regulatory landscape surrounding blockchain-based document verification systems and its impact on adoption and implementation. It analyzes the legal and compliance considerations relevant to document

verification processes, including data privacy regulations, intellectual property rights, and cross-border legal frameworks. Moreover, the survey investigates the role of standards bodies, industry consortia, and governmental agencies in establishing guidelines and best practices for blockchain-based verification systems. Furthermore, it discusses the challenges and opportunities associated with regulatory compliance in decentralized environments, such as jurisdictional conflicts, enforcement mechanisms, and liability issues. By addressing the regulatory aspects of blockchain-based document verification, this survey seeks to provide insights into the legal and policy implications shaping the adoption and deployment of blockchain technology in verification processes. The survey explores emerging trends and innovations in blockchain technology that have the potential to further enhance document verification processes.

* 1. **ENHANCING DIGITAL COPYRIGHT MANAGEMENT WITH BLOCKCHAIN AUTHOR:** Wang, L. et al. (2021)

## DESCRIPTION:

The literature survey on "Enhancing Digital Copyright Management with Blockchain" provides a comprehensive examination of the research, developments, and applications related to leveraging blockchain technology for managing digital copyright in various industries.

The survey begins by exploring the challenges and limitations of traditional copyright management systems, particularly in the digital domain. It discusses issues such as copyright infringement, piracy, unauthorized distribution, and lack of transparency in tracking ownership and usage rights. Furthermore, the survey delves into the fundamental principles of blockchain technology and its potential to address these challenges in digital copyright management. It examines how blockchain's decentralized, transparent, and immutable nature can provide a robust infrastructure for tracking and enforcing copyright ownership, usage rights, and royalty payments.

Moreover, the survey delves into the challenges and barriers to the widespread adoption of blockchain technology in digital copyright management. It considers factors such as scalability limitations, interoperability issues, regulatory uncertainties, and the need for industry-wide collaboration and standardization efforts.

Additionally, the survey evaluates the potential benefits and implications of adopting blockchain technology for digital copyright management. It considers factors such as increased security, transparency, efficiency, and fairness in royalty distribution, as well as the potential impact on stakeholders such as content creators, publishers, distributors, and consumers.

Additionally, the survey examines emerging trends and innovations in blockchain-based digital copyright management, such as the integration of decentralized identity and verifiable credentials for copyright attribution and licensing, the tokenization of intellectual property rights for fractional ownership and investment, and the use of non-fungible tokens (NFTs) for representing unique digital assets and collectibles. It assesses the potential impact of these developments on the future landscape of digital content creation, distribution, and monetization.

Overall, this literature survey serves as a comprehensive guide for researchers, practitioners, and policymakers interested in understanding the potential of blockchain technology for enhancing digital copyright management. By synthesizing existing research findings, identifying key challenges and opportunities, and offering insights into emerging trends and innovations, the survey aims to contribute to the advancement of blockchain-based solutions in this critical area of intellectual property management. Furthermore, the survey dives into the societal and cultural implications of blockchain-based digital copyright management, considering factors such as democratization of access to content, preservation of cultural heritage, and empowerment of marginalized creators and communities. It explores the role of blockchain in promoting inclusivity, diversity, and equitable representation in the digital content landscape, and assesses its potential to reshape power dynamics within the creative industries.

In conclusion, this expansive literature survey represents a seminal contribution to the burgeoning field of blockchain-based digital copyright management. By delving into the technical, regulatory, economic, and societal dimensions of blockchain implementations in copyright management, the survey offers a holistic understanding of the opportunities, challenges, and implications of harnessing blockchain technology .

## BLOCKCHAIN-BASED DOCUMENT VERIFICATION: CHALLENGES AND OPPORTUNITIES

**AUTHOR:** Kim, S. et al.

## DESCRIPTION:

The literature survey on "Blockchain-Based Document Verification: Challenges and Opportunities" offers a comprehensive analysis of the research, trends, and advancements in utilizing blockchain technology for document verification purposes. The

survey investigates the potential of blockchain to revolutionize document verification processes by providing a secure, transparent, and tamper-proof infrastructure.

The survey begins by examining the fundamental principles of blockchain technology and its relevance to document verification. It explores how blockchain's decentralized and immutable nature can address the shortcomings of

traditional verification methods, such as reliance on centralized authorities and susceptibility to tampering.

Furthermore, the survey delves into various blockchain-based document verification systems and their implementation in different domains. It discusses the design principles, architectural components, and functionalities of these systems, highlighting their key features and advantages over conventional approaches.

Moreover, the survey evaluates the challenges and limitations associated with deploying blockchain technology for document verification. It discusses issues such as scalability, interoperability, regulatory compliance, and user adoption, offering insights into potential solutions and future research directions.

Additionally, the survey identifies the opportunities and potential benefits of adopting blockchain-based document verification systems. It considers factors such as increased security, data integrity, transparency, and efficiency in document

verification processes, as well as the potential impact on various industries such as

finance, healthcare, legal, and supply chain management.

Furthermore, the survey examines real-world use cases and case studies of blockchain technology being applied to document verification. It assesses the effectiveness of blockchain-based solutions in addressing verification-related challenges and improving the overall reliability and trustworthiness of document verification processes.

Overall, this literature survey aims to provide a comprehensive overview of the current state-of-the-art in utilizing blockchain technology for document verification. It synthesizes existing research findings, identifies challenges and

opportunities, and offers recommendations for future research and practical implementations in this rapidly evolving field.

## CHAPTER 3 SYSTEM ANALYSIS

* 1. **EXISTING SYSTEM**

The traditional system for document verification relies on centralized authorities or intermediaries to authenticate and verify the validity of documents, which typically involves manual processes and paper-based documentation. In this system, government agencies, educational institutions, legal authorities, or other centralized entities maintain records of verified documents and issue official seals or stamps to authenticate them. Document verification often entails physical inspection, comparison of document details with records, and verification of signatures or seals. However, these processes can be time- consuming, labor-intensive, and prone to errors. Documents are usually stored and transmitted in paper format, which exposes them to risks such as forgery, tampering, and unauthorized access. Moreover, access to document verification services may be limited by geographical location or administrative barriers. These challenges highlight the need for innovative solutions to enhance the security, efficiency, and accessibility of document verification processes.

### Disadvantages

* + - * Reliance on centralized authorities.
      * Manual verification processes prone to human error.
      * Security risks associated with paper-based documentation, such as forgery and tampering

## PROPOSED SYSTEM

The proposed system for document verification aims to revolutionize the current practices by leveraging blockchain technology's decentralized, transparent, and tamper-proof ledger. Unlike the centralized authorities or intermediaries in the traditional system, this system utilizes a decentralized network of computers (nodes) to store and verify documents. Each document undergoes cryptographic hashing and is added to a shared blockchain ledger, ensuring transparency and immutability. This immutable record-keeping feature guarantees the integrity and authenticity of documents, mitigating risks associated with forgery, tampering, or unauthorized access. Furthermore, the verification process is transparent and auditable, enabling stakeholders to track document transactions and verify their authenticity in real-time. Smart contracts, which are self-executing contracts with predefined terms written in code, automate document verification processes on the blockchain. They can enforce rules and conditions for verification, such as verifying the identity of the document issuer or validating signatures. Enhanced security and privacy are ensured through blockchain's cryptographic techniques, including public-key cryptography for securing document ownership and zero-knowledge proofs for verifying authenticity without disclosing sensitive information. Moreover, the proposed system offers global accessibility to document verification services, enabling individuals and organizations to securely verify documents from anywhere in the world. In summary, the proposed system for document verification using blockchain provides a decentralized, transparent, and secure alternative to the traditional system, with the potential to revolutionize document verification processes.

### Advantages

* + - * Decentralized infrastructure ensures transparency and reduces reliance on centralized authorities.
      * Immutable record-keeping on the blockchain ledger ensures the integrity and authenticity of documents.
      * Transparent verification process allows stakeholders to track document transactions in real-

time.

* + - * Smart contracts automate document verification processes, reducing manual intervention and errors.
      * Enhanced security and privacy through blockchain's cryptographic techniques.
      * Global accessibility enables individuals and organizations to verify documents securely from anywhere.

## CHAPTER 4 SYSTEM REQUIREMENTS

## 4.1 HARDWARE REQUIREMENTS

* CPU type: Mid Range – CPU Intel i5
* Clock speed: 3.0 GHz with multiple cores
* Ram size: 8GB
* Hard disk capacity: 1000GB

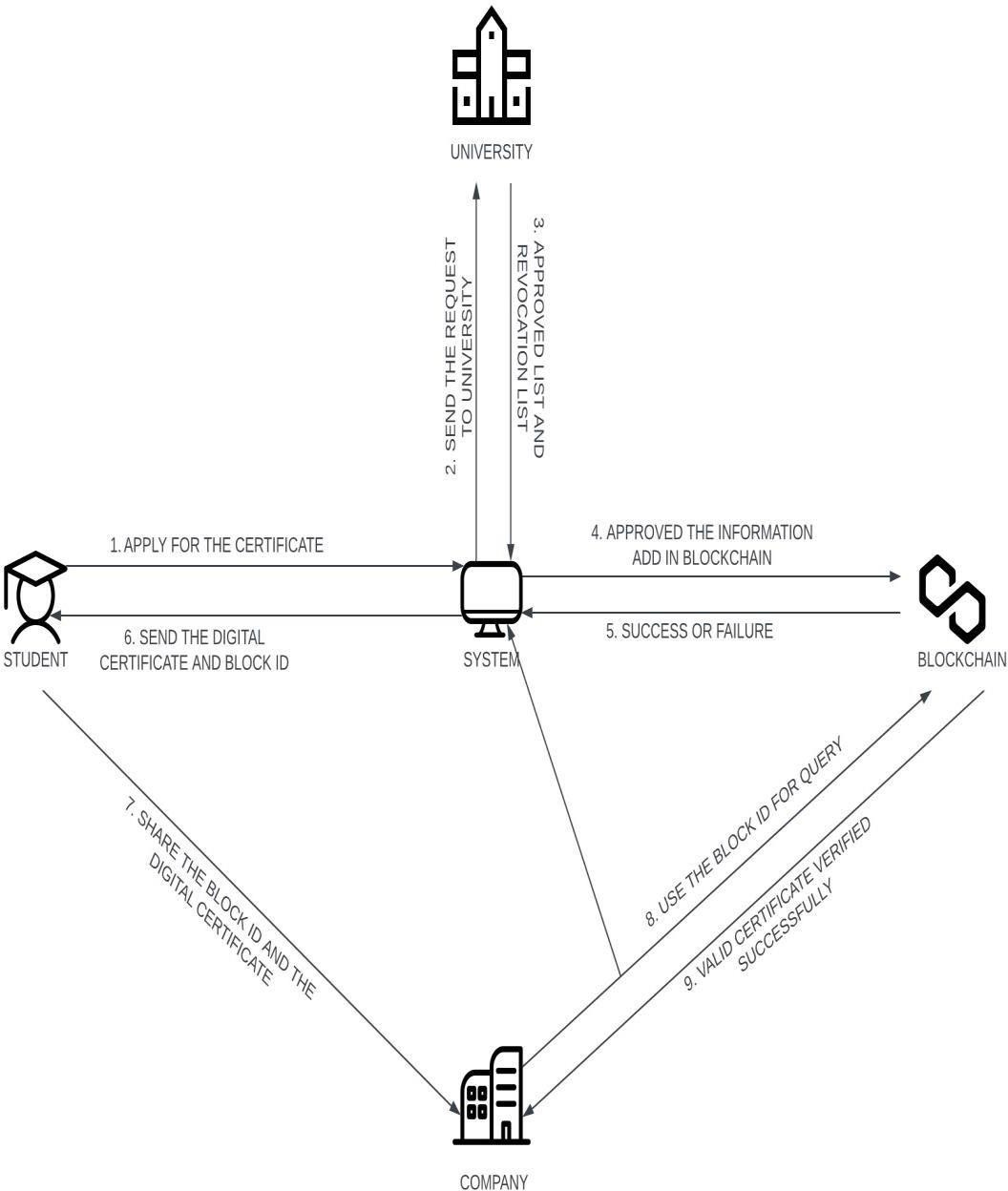
**4.2 SOFTWARE REQUIREMENTS**

* Ganache
* IPFS
* Metamask
* Node.Js
* Operating System : Windows OS

# CHAPTER 5 SYSTEM DESIGN

## SYSTEM ARCHITECTURE

The system architecture for the blockchain-based document verification system encompasses several interconnected components designed to facilitate secure and efficient document verification processes. At its core, the system includes a user interface providing a user-friendly platform for individuals and organizations to interact with the system. Users can upload documents for verification, access verification results, and manage document-related tasks through this interface. The document verification module processes verification requests submitted by users, leveraging the blockchain network for validation. The blockchain network, composed of decentralized nodes, maintains a shared ledger of verified documents, ensuring transparency and immutability. Smart contracts, encoded with predefined terms and conditions, automate verification processes on the blockchain, enforcing rules for document authenticity and access control. Additionally, cryptographic techniques such as hash functions, digital signatures, and zero-knowledge proofs are utilized to enhance security and privacy. A database component may be integrated to store metadata and document-related information, enabling efficient querying and retrieval. Integration interfaces facilitate seamless interoperability with external systems and services, while a dedicated security layer safeguards the system against potential threats. Together, these components form a robust and scalable system architecture designed to provide a secure, transparent, and user- centric solution for document verification using blockchain technology.



**Fig 5.1: System Architecture**

## DATAFLOW DIAGRAM

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data

to the system, various processing carried out on this data, and the output data is

generated by this system.

1. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are

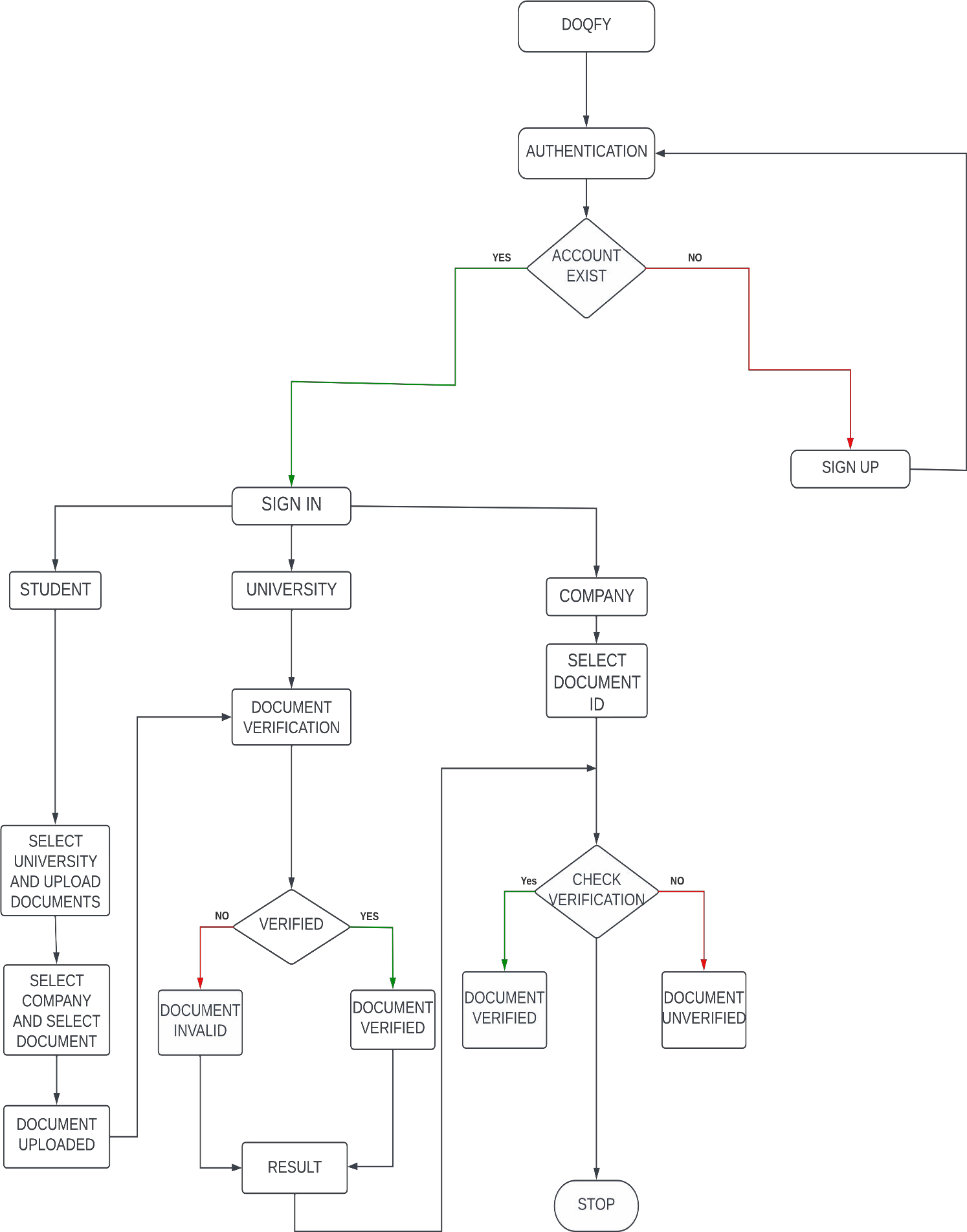
the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

1. DFD shows how the information moves through the system and how it modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data from input to output.

is

moves

1. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.



**Fig No 5.2: Dataflow Diagram**

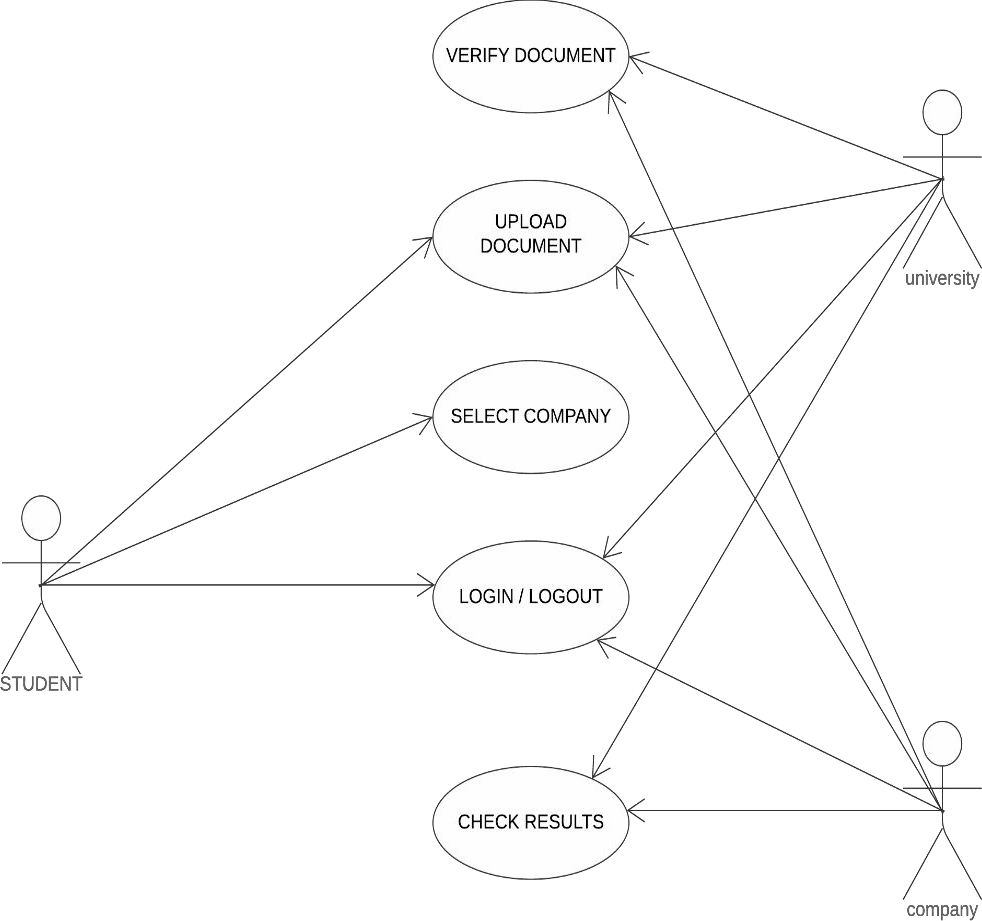
## USE CASE DIAGRAM

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

The document verification system involves three main actors: the User, the Verifier, and the Blockchain Network. The User interacts with the system by submitting documents for verification. Upon submission, the system validates the document's format and authenticity requirements, creates metadata, and generates a hash of the document. These details are then added to the blockchain for secure storage and

verification. The Verifier, on the other hand, utilizes the system to verify the authenticity of documents. They initiate a request to verify a specific document, which prompts the system to retrieve the document's record from the blockchain. The Verifier compares the

document metadata and hash with the submitted document to confirm or reject its authenticity. Additionally, users have the capability to view the verification history of documents they've submitted. By selecting a document, the system retrieves its verification history from the blockchain, presenting a chronological list of verification events. Verifiers also have the ability to update the status of document verifications, providing feedback or status updates which are recorded in the blockchain. Lastly, the Blockchain Network itself audits document records periodically to ensure consistency and integrity. Any inconsistencies or suspicious activities are flagged for further investigation, maintaining the system's security and reliability.



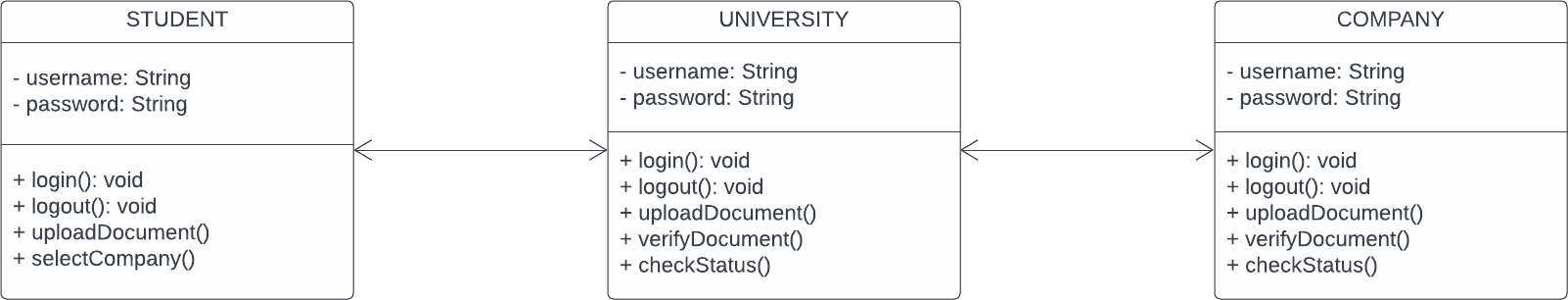
**Fig No 5.3: Use Case Diagram**

## CLASS DIAGRAM

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

The class diagram outlines the key components of the document verification system using blockchain. At its core is the "Document" class, which encapsulates attributes such as document ID, title, content, owner, hash, and verification status. Each

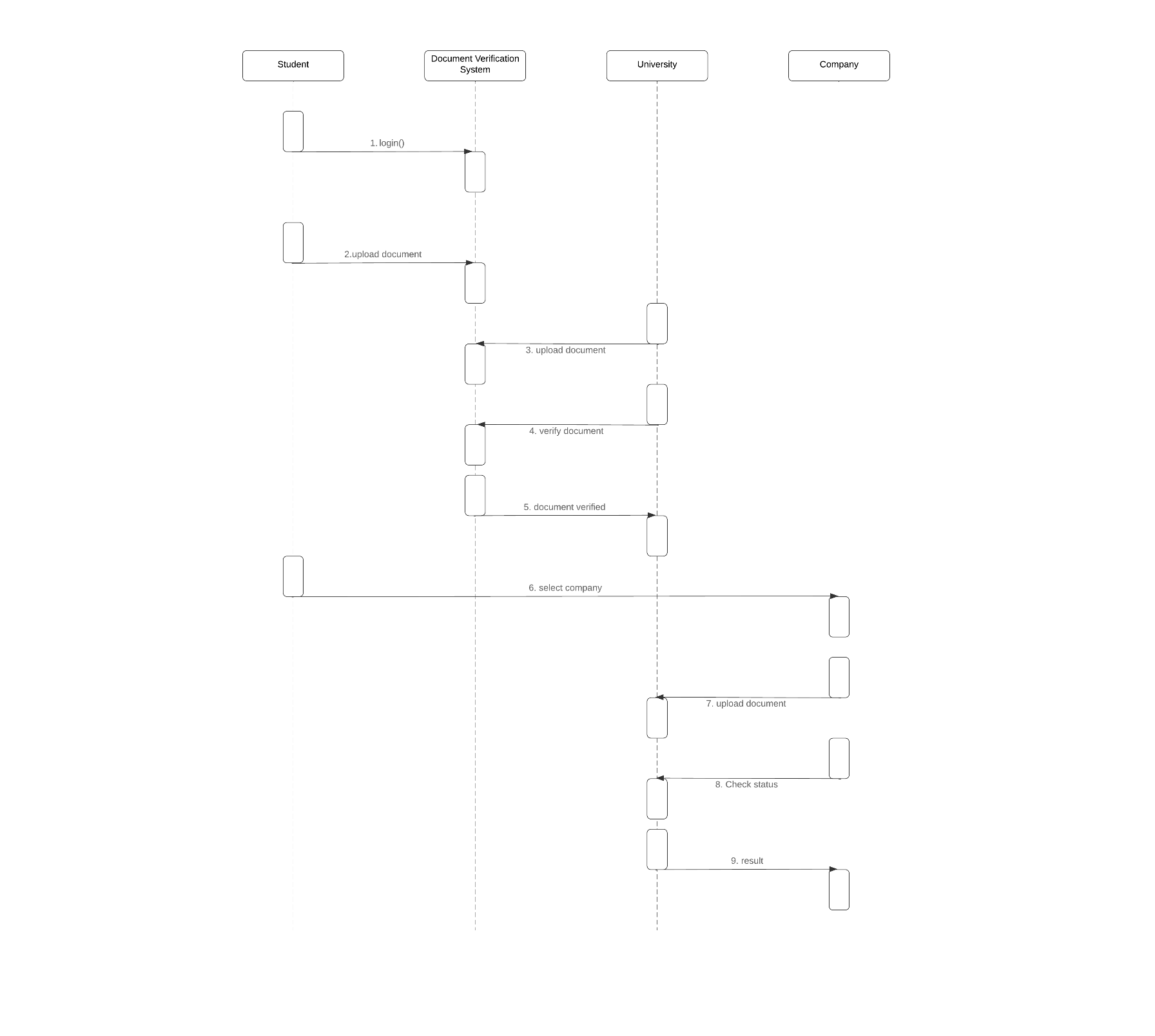
document can be uploaded, verified, and have its verification status updated through corresponding methods. Users interact with the system via the "User" class, which represents individuals with attributes including user ID, username, and email. The "Blockchain Network" class manages the decentralized network where document records are stored and verified. It maintains a list of nodes within the network and offers functionality to add and remove nodes, as well as to verify document authenticity. Each node in the network is represented by the "Node" class, featuring attributes like node ID, IP address, and port number. This class facilitates the communication and coordination among nodes within the blockchain network. Together, these classes form the backbone of the document verification system, enabling secure and transparent verification. This diagram demonstrates the interactions between actors (students, companies, and universities) and the system, facilitating document verification processes. Each class encapsulates its specific functionalities, ensuring a modular and organized design for the document verification system.



**Fig No 5.4: Class Diagram**

## SEQUENCE DIAGRAM

The sequence diagram illustrates the sequential interactions among the actors (Student, Company, University) and the Document Verification System. Beginning with the Student, the sequence initiates with the login action, where the student authenticates themselves to the system. Subsequently, the student uploads a document for verification, triggering the verification process within the Document Verification System. This process involves interaction with the University, which verifies the document. Once verified, the Document Verification System provides the verification result back to the student, who then logs out of the system. Similarly, the Company and University actors also undergo login procedures before engaging with the Document Verification System. After successful authentication, they perform their respective actions, such as verifying documents or viewing verification results. Once their tasks are completed, they log out of the system. This sequential representation elucidates the step-by-step flow of interactions between actors and the system, outlining the authentication, document verification, and result retrieval process



**Fig No 5.5: Sequence Diagram**

# CHAPTER 6 MODULE DESCRIPTION

* 1. **LIST OF MODULES**

1. Decentralized User Registration Module
2. Identity Verification Module
3. Student Identity Vault Module
4. Credential Forge Module
5. Hire Guard Module

### Decentralized User Registration Module

The Decentralized User Registration Module serves as a pivotal component within the blockchain-based document verification system, facilitating the seamless onboarding of users onto the platform. Unlike traditional centralized user registration systems, which rely on a single authority or intermediary to manage user accounts and credentials, the decentralized nature of this module ensures greater transparency, security, and user autonomy.

|  |  |  |
| --- | --- | --- |
| At its core, the module leverages | the inherent | capabilities of |
| blockchain technology to enable users to register | and manage | their identities |

autonomously, without the need for intermediaries or third-party service providers. Users retain full control over their personal information and authentication credentials, which are securely stored and managed on the blockchain network.

The registration process begins with users generating a unique cryptographic key pair consisting of a public key and a private key. The public key serves as their identity on the blockchain network, while the private key is used to authenticate and authorize transactions associated with their identity. Users then submit their public key along with any additional registration information to the blockchain network, where it is recorded and verified by network nodes.

Upon successful registration, users are granted access to their decentralized identity, which can be used to interact with various services and applications within the ecosystem. This decentralized identity serves as a secure and tamper-proof representation of the user's credentials, eliminating the need for traditional username-password combinations and reducing the risk of identity theft or unauthorized access.

Furthermore, the Decentralized User Registration Module incorporates robust encryption and cryptographic protocols to ensure the confidentiality and integrity of user data throughout the registration process. Users' personal information is encrypted and stored in an immutable and tamper-proof manner on the blockchain ledger, protecting it from unauthorized access or manipulation.

Overall, the Decentralized User Registration Module plays a critical role in fostering a secure, transparent, and user-centric environment within the blockchain-based document verification system. By empowering users to control their own identities and registration information, it lays the foundation for a decentralized ecosystem built on trust, integrity, and user empowerment.

### Identity Verification Module

The Identity Verification Module serves as a cornerstone component within the blockchain-based document verification system, facilitating the secure and reliable verification of user identities. In today's digital landscape, establishing trust and authenticity in online interactions is paramount, and the Identity Verification Module addresses this challenge by leveraging advanced technologies and cryptographic techniques to verify users' identities with confidence and accuracy.

At its essence, the module employs a multifaceted approach to identity verification, combining biometric data, government-issued identification documents, and blockchain-based attestations to establish the authenticity of users' identities. Upon registration, users are required to provide a combination of biometric identifiers such as fingerprints, facial recognition scans, or voice prints, along with government-issued identification documents such as passports, driver's licenses, or national identification cards.

Once submitted, this information undergoes rigorous verification and validation processes to ensure its accuracy and integrity. Biometric data is compared against existing records to verify the user's physical identity, while government-issued identification documents are authenticated using advanced optical character recognition (OCR) technology and document verification algorithms.In addition to biometric and document-based verification, the module incorporates blockchain-based attestations to further enhance the reliability and trustworthiness of user identities. Users have the option to request attestations from trusted third-party entities such as government agencies, financial institutions, or educational institutions, which are then cryptographically signed and recorded on the blockchain ledger. These attestations serve as verifiable proof of the user's identity and can be independently verified by any party with access to the blockchain network.

Furthermore, the Identity Verification Module employs robust encryption and cryptographic protocols to safeguard user data and ensure its confidentiality and integrity throughout the verification process. Personal information and biometric data are encrypted and stored in a decentralized and tamper-proof manner on the blockchain ledger, protecting it from unauthorized access or manipulation.

Overall, the Identity Verification Module plays a pivotal role in establishing trust, security, and integrity within the blockchain-based document verification system. By combining advanced biometric technologies, government- issued identification documents, and blockchain-based attestations, it provides a robust framework for verifying user identities with confidence and accuracy in today's digital age.

By leveraging blockchain technology, academic transcripts can be securely shared and verified in real-time, reducing administrative overhead, eliminating the risk of tampering or falsification, and facilitating seamless transfer of academic credits and qualifications between institutions. This feature promotes interoperability and collaboration within the education ecosystem, empowering students to seamlessly transition between educational programs and institutions while maintaining the integrity and authenticity of their academic records.

### Student Identity Vault Module

The Student Identity Vault Module is a pivotal component within the blockchain-based document verification system, specifically designed to securely

manage and authenticate student identities and academic credentials. As educational institutions increasingly embrace digitalization, the need for a reliable and tamper-proof

system to verify student identities and academic achievements becomes paramount. The Student Identity Vault Module addresses this need by providing a secure and immutable repository for storing and managing student identity information, academic records, and certifications on the blockchain.

At its core, the module leverages blockchain technology to create a decentralized and transparent ledger of student identities and academic credentials. Each student is assigned a unique cryptographic identifier, which serves as their digital identity on the blockchain network. This identifier is securely linked to their academic records, including transcripts, diplomas, certificates, and other relevant documents, ensuring their authenticity and integrity.

The Student Identity Vault Module offers several key features to enhance the security, accessibility, and usability of student identity and academic credential management. Firstly, it employs robust encryption and cryptographic hashing techniques to protect student data from unauthorized access or tampering. All student information and academic records stored in the vault are encrypted and immutable, providing a high level of security and integrity.

Secondly, the module provides seamless integration with educational institutions' existing systems and platforms, allowing for easy and efficient data exchange. Through standardized APIs and data formats, the module enables interoperability with student information systems (SIS), learning management systems(LMS), and other educational software solutions, ensuring a smooth and frictionless user experience for students, faculty, and administrators alike.

Furthermore, the Student Identity Vault Module offers advanced

verification capabilities, allowing employers, academic institutions, and other third parties to independently verify the authenticity of student identities and academic credentials. Through cryptographic signatures and attestations recorded on the blockchain.

### Credential Forge Module

The Credential Forge Module is a vital component within the blockchain-based document verification system, designed to ensure the secure and reliable issuance of digital credentials and certificates. In today's digital landscape, the demand for verifiable and tamper-proof credentials is increasing, as individuals seek to authenticate their skills, qualifications, and achievements in various domains. The Credential Forge Module addresses this need by providing a robust framework for educational institutions, certification authorities, and other organizations to securely issue and manage digital credentials on the blockchain. At its core, the module leverages blockchain technology to create a decentralized and immutable ledger of digital credentials and certificates. Educational institutions, certification authorities, and other issuers can utilize the module to generate unique digital credentials for students, professionals, and individuals, which are securely recorded and stored on the blockchain network. These digital credentials encompass a wide range of achievements, including academic degrees, professional certifications, licenses, and endorsements, each represented as a tamper-proof digital asset on the blockchain.

The Credential Forge Module offers several key features to streamline the credential issuance process and enhance the security and integrity of digital credentials. Firstly, it provides customizable templates and frameworks for issuers to create and customize digital credential formats according to their specific requirements

and standards. Whether issuing academic diplomas, professional certificates, or industry credentials, issuers can tailor the credential design, content, and metadata to meet their unique needs.

Secondly, the module employs advanced cryptographic techniques and digital signatures to ensure the authenticity and integrity of digital credentials. Each credential is cryptographically signed by the issuer and recorded on the blockchain ledger, providing a verifiable proof of its origin and authenticity. This cryptographic assurance eliminates the risk of credential forgery, tampering, or unauthorized modification, enhancing trust and confidence in the credential verification process.

Furthermore, the Credential Forge Module supports interoperability and compatibility with existing credentialing systems and standards, allowing issuers to seamlessly integrate digital credentials into their existing workflows and processes. Through standardized APIs, data formats, and protocols, issuers can exchange digital credentials with other systems, platforms, and stakeholders, facilitating the seamless sharing and verification of credentials across different domains and applications.

Overall, the Credential Forge Module empowers issuers to securely issue and manage digital credentials with confidence and ease, while providing recipients with verifiable proof of their achievements and qualifications. By harnessing the power of blockchain technology, it revolutionizes the credentialing process, offering a secure, transparent, and tamper-proof solution for issuing, sharing, and verifying digital credentials in today's digital economy.

### Hire Guard module

The Hire Guard Module is a pivotal component within the proposed blockchain-based document verification system, dedicated to ensuring the authenticity

and integrity of employment-related documents and credentials. In today's digital landscape, the verification of employment documents, such as resumes, certifications,

and background checks, is crucial for employers to make informed hiring decisions and

mitigate the risk of fraudulent activities. The Hire Guard Module addresses these challenges by leveraging blockchain technology to provide a secure and transparent platform for verifying the authenticity of employment-related documents and credentials.

At its core, the Hire Guard Module acts as a trusted intermediary between job seekers and employers, facilitating the seamless verification of employment documents and credentials. Job seekers can securely upload their employment-related documents to the platform, including resumes, diplomas, certifications, and references, which are then stored securely on the blockchain ledger. Each document is encrypted and timestamped, ensuring its integrity and immutability. Employers, on the other hand, can access the Hire Guard Module to verify the authenticity of job seekers' employment documents and credentials during the hiring process. Through a user-friendly interface, employers can request access to specific documents or credentials from job seekers, which are then retrieved from the blockchain ledger and presented to the employer for verification. Employers can verify the authenticity of the documents using cryptographic techniques and digital signatures, providing them with assurance that the documents have not been tampered with or falsified

The Hire Guard Module offers several key features to enhance the efficiency and reliability of employment document verification. Firstly, it provides real- time verification capabilities, allowing employers to instantly verify the authenticity of documents and credentials without the need for manual intervention or third-party verification services. This reduces the time and cost associated with traditional

verification processes and enables employers to make faster hiring decisions.

Secondly, the module incorporates advanced security measures to protect sensitive employment-related information and ensure the privacy of job seekers. Employers are granted access to only the documents and credentials that they have requested, while job seekers retain control over their personal information and can choose which documents to share with prospective employers. Additionally, the use of blockchain technology ensures that all transactions and interactions within the platform are secure, transparent, and tamper-proof.

Overall, the Hire Guard Module serves as a trusted and reliable platform for verifying employment-related documents and credentials, empowering employers to make informed hiring decisions and ensuring the integrity and authenticity of their workforce. By leveraging blockchain technology, the module provides a secure, transparent, and efficient solution for document verification in the hiring process, enhancing trust and confidence among employers and job seekers alike.

# CHAPTER 7

**CONCLUSION AND FUTURE ENHANCEMENT**

## CONCLUSION

modules,

Throughout the project, we have explored and implemented various including the Decentralized User Registration, Identity Verification,

Credential Forge, Hire Guard, and Student Identity Vault modules, each contributing to different aspects of the document verification process. These modules empower users to securely manage their identities and credentials, facilitate the issuance and verification of digital credentials, and safeguard against fraudulent activities in the hiring process.

Looking ahead, the project presents several opportunities for future enhancement and development, including the integration of AI and machine learning technologies, enhancement of privacy features, optimization of scalability and performance, expansion of use cases, and continuous improvement of the user experience. These future enhancements will further strengthen the capabilities and relevance of the project in addressing emerging challenges and meeting the evolving needs of businesses, institutions, and individuals in an increasingly digital world.

In conclusion, the project on "Document Verification Using Blockchain" underscores the transformative potential of blockchain technology in revolutionizing document management and verification processes, paving the way for a more secure,

transparent, and efficient digital ecosystem. As organizations continue to embrace digital transformation, the adoption of blockchain-based document verification systems will play a crucial role in shaping the future of document management and authentication.

## FUTURE ENHANCEMENT

While the proposed blockchain-based document verification system offers robust functionality and security, there are several areas for future enhancement and development to further improve its capabilities and address emerging challenges in document management and verification:

1. **Integration with AI and Machine Learning**: Incorporating artificial intelligence (AI) and machine learning (ML) algorithms can enhance the system's ability to detect and prevent document fraud and manipulation. AI-powered image recognition and pattern recognition technologies can help identify forged documents or altered credentials with greater accuracy and efficiency.
2. **Enhanced Privacy Features**: Introducing advanced privacy features, such as zero-knowledge proofs and homomorphic encryption, can further enhance the privacy and confidentiality of user data within the system. These cryptographic techniques allow for secure data sharing and verification without revealing sensitive information.
3. **Interoperability with Existing Systems**: Enhancing interoperability with existing document management systems, identity verification platforms, and credentialing services can streamline integration and adoption of the blockchain-based verification system across different industries and domains. Standardized APIs and data formats facilitate seamless data exchange and collaboration with external systems and services.
4. **Scalability and Performance Optimization**: As the volume of documents and users within the system grows, optimizing scalability and performance becomes essential. Implementing sharding techniques, layer-two scaling solutions, and consensus algorithms tailored for high-throughput environments can ensure the system can handle increased transaction volumes and maintain optimal performance**.**
5. **Expansion of Use Cases**: While the system primarily focuses on document verification for employment and education purposes, exploring additional use cases and applications can expand its utility and relevance. For example, extending the system to verify medical records, legal documents, or supply chain documents can address broader societal and business needs.
6. **Enhanced User Experience**: Continuously improving the user interface and experience based on user feedback and usability studies can enhance user adoption and satisfaction. Intuitive interfaces, clear instructions, and seamless workflows contribute to a positive user experience and encourage broader adoption of the system.
7. **Regulatory Compliance**: Ensuring compliance with evolving regulatory requirements and data protection laws, such as GDPR, HIPAA, and CCPA, is crucial for maintaining trust and credibility. Regular audits, compliance checks, and updates to the system's policies and procedures help ensure adherence to relevant regulations and standards.

# APPENDICES

# APPENDIX:1

**SAMPLE CODE**

**AuthPage.jsx:**

import React, { useState, useEffect, useRef } from 'react';

//import { Button, Select, Input, Option } from "@material-tailwind/react"; import { useForm, Controller } from 'react-hook-form';

import { motion, AnimatePresence } from 'framer-motion';

//import { ChevronLeftIcon, ChevronRightIcon } from '@heroicons/react/24/solid';

//import { FaChevronLeft,FaChevronRight } from "react-icons/fa6"; import { HiChevronLeft ,HiChevronRight } from "react-icons/hi"; import { useNavigate, useParams } from 'react-router-dom';

import { useUserContext } from '../context/UserContext';

import axios from 'axios';

import { useMetaMaskContext } from '../context/MetaMaskContext'; import {

Box, Button, Flex, Icon,

IconButton, Select, Stack, Step,

StepDescription, StepIcon, StepIndicator, StepNumber, StepSeparator, StepStatus, StepTitle, Stepper,

useColorModeValue, useSteps,

} from '@chakra-ui/react'

import Card from '../components/card/Card';

import IconBox from '../components/icons/IconBox'; import InputField from '../components/fields/InputField'; import { toast, ToastContainer } from 'react-toastify';

import "react-toastify/dist/ReactToastify.css"; import { IoMdLogIn } from "react-icons/io"; import { IoMdLogOut } from "react-icons/io"; import { MdError } from "react-icons/md";

import { IoMdCloseCircle } from "react-icons/io";

import playToastSound from '../mainComponents/ToastSound'; const AuthPage = () => {

const { type } = useParams();

const { account } = useMetaMaskContext(); const navigate = useNavigate();

const { control, setValue, register, handleSubmit, formState: { errors }, watch } = useForm();

const selectedRole = watch('role');

const [isLogin, setLogin] = useState(false); const { login } = useUserContext();

const cardbg = useColorModeValue('#ffffff', 'navy.800');

const brandColor = useColorModeValue("brand", "white");

const boxBg = useColorModeValue("secondaryGray.300", "whiteAlpha.100"); const disabledColor = useColorModeValue('secondaryGray.400', 'navy.900');

const onSubmit = async (data) => { const userData = isLogin

? { role: data.role, email: data.email, password: data.password, address: data.address }

: { role: data.role, name: data.name, email: data.email, password: data.password, roleid: data.roleid, address: data.address };

const apiEndpoint = isLogin ? 'login' : 'signup'; console.log(isLogin ? 'login:' : 'signup:', data.role, userData);

try {

const response = await axios.post(`http://localhost:5000/auth/${apiEndpoint}`,

userData);

<IconButton ml='7' fontSize='0px' icon={<HiChevronRight className='h-7 w- 7' />} color={brandColor} bg={boxBg} onClick={handleNext} isDisabled={isLastStep ||

!selectedRole} isRound='true' />

</Box>

</Box>

</Box>

);

};

export default AuthPage;

### CompanyPage.jsx:

import React, { useState, useEffect, useContext, useCallback } from 'react'; import { useMetaMaskContext } from '../context/MetaMaskContext';

import axios from 'axios';

import { useLocation } from 'react-router-dom';

import MiniStatistics from '../components/card/MiniStatistics'; import IconBox from '../components/icons/IconBox';

import {Text, Box, Button, Flex, Icon, SimpleGrid, Stack, useColorModeValue } from '@chakra-

ui/react';

import { FaRegAddressBook } from "react-icons/fa"; import { MdOutlineVerified } from "react-icons/md";

import { Table, Tbody, Tr,Th,Td,

} from '@chakra-ui/react'

import {

MdFileCopy,

} from "react-icons/md";

import { FaBuilding } from "react-icons/fa"; import { MdCancel } from "react-icons/md";

import FileUpload from '../mainComponents/FileUpload';

import { toast } from 'react-toastify';

import "react-toastify/dist/ReactToastify.css"; import { IoMdCloseCircle } from "react-icons/io";

import playToastSound from '../mainComponents/ToastSound';

// Create a Web3 instance using the current Ethereum provider (MetaMask)

function CompanyPage() {

const [file, setFile] = useState(null);

const [status, setStatus] = useState(''); //check n verify status//

const [QrCodeText, setQrCodeText] = useState(''); //input box and path qr txt// const { contract, account } = useMetaMaskContext();

const location = useLocation();

const [isCompanyVerified, setIsCompanyVerified] = useState(true);

const [DocumentDetails, setDocumentDetails] = useState(null); //check status//

try {

// Call the smart contract function

const transaction = await contract.registerCompany({ from: account }); await transaction.wait();

console.log('Company registered successfully:', transaction);

toast.success(`Company registered successfully`, { icon: FaBuilding,

onOpen: () => {

playToastSound(); // Play the sound when the toast opens

},

});

} catch (error) {

console.error('Error registring company:', error.reason); toast.error('Error registring company', {

icon: IoMdCloseCircle,

onOpen: () => {

playToastSound(); // Play the sound when the toast opens

},

});

// Handle the error here

}

}

async function checkCompany() { try {

// Call the smart contract function

const transaction = await contract.checkCompany(account, { from: account }); setIsCompanyVerified(transaction);

console.log('Company status:', transaction);

} catch (error) {

console.error('Error checking company:', error.reason);

// Handle the error here

}

}

const handleChange = (event) => { setQrCodeText(event.target.value);

};

useEffect(() => {

// Check if contract is not null if (contract !== null) { checkCompany();

}

}, [account]);

const cellStyle = { wordBreak: 'break-all', padding: '5px',

cursor: 'pointer', // Adding a pointer cursor to indicate clickable content

};

const handleCopyToClipboard = (text) => { navigator.clipboard.writeText(text)

.then(() => {

// Notify the user or handle success if needed

// console.log('Text copied to clipboard:', text); toast.success('Text copied to clipboard', { icon: MdFileCopy,

});

})

.catch((error) => {

// Handle error if clipboard write fails console.error('Failed to copy text to clipboard:', error);

});

};

</Tr>

</Tbody>

</Table>

</Box>

</>

}

</Stack>

: null}

</SimpleGrid>

</Box>

);

}

export default CompanyPage;

### UniversityPage.jsx:

const { contract, account } = useMetaMaskContext();

const [companyAddresses, setCompanyAddresses] = useState([]);

const [selectedCompany, setSelectedCompany] = useState(''); // State for selected company address

const [universityDocumentlist, setUniversityDocumentlist] = useState([]); // State for selected company address

const [selectedUUID, setSelectedUUID] = useState(''); // State for selected company address

const [DocumentCompanylist, setDocumentCompanylist] = useState([]); // State for selected company address

const [DocumentDetails, setDocumentDetails] = useState([]); // State for selected company

// Call the smart contract function

const transaction = await contract.unverifyDocument(selectedUUID, \_newcid, { from:

account });

await transaction.wait(); setTransaction(transaction);

console.log('Document unVerified successfully:', transaction);

getUniversityDocumentList();

toast.success(' Document un-verified Successfully', { icon:MdOutlineVerified,

onOpen: () => {

playToastSound(); // Play the sound when the toast opens

},

});

} catch (error) {

};

async function includeCompany() { try {

setIpfsData(null); setTransaction(null);

// Call the smart contract function

const transaction = await contract.includeCompany(selectedUUID, selectedCompany, { from:

account });

await transaction.wait(); setTransaction(transaction);

getDocumentCompanyList(selectedUUID); console.log('Company included successfully:', transaction); toast.success('Company included Successfully', { icon:FaBuilding,

onOpen: () => {

playToastSound(); // Play the sound when the toast opens

},

});

<SimpleGrid columns={{ base: 1, md: 2, xl: 2 }} gap='20px' mb='20px'>

{/\* add or remove company \*/}

<CompanyManage handleDocumentChange={handleDocumentChange} uuid={selectedUUID} Documentlist={universityDocumentlist}

handleCompanyChange={handleCompanyChange}

selectedCompany={selectedCompany}

companyAddresses={companyAddresses} includeCompany={includeCompany} removeCompany={removeCompany}

/>

{/\* Document Companies List \*/}

<TabelCard data={[DocumentCompanylist]} headers={["S.N", "Companies"]} heading={"Document Companies List"} searchId={0} searchLabel={"Search Company"}

/>

</SimpleGrid>

<SimpleGrid columns={{ base: 1, md: 1, xl: 1 }} gap='20px' mb='20px' >

{/\* Company Document List \*/}

<TabelCard data={DocumentDetails} headers={["S.N", "Document", "Student", "IPFS CID", "Verified"]}

heading={"Company Document List"} searchId={1} searchLabel={"Search Document"}

/>

</SimpleGrid>

</Box>

);

}

export default UniversityPage;

### Contract.sol:

Document memory document = Document({ owner: msg.sender, universityAddress: universityAddress, ipfsHash: ipfsHash,

verified: false

});

documentsById[uniqueId] = document; // Store the document by its id // universityDocumentList[universityAddress].push(uniqueId); //add new id in university

document list

studentDocumentList[msg.sender].push(uniqueId); //add new id in student document list emit LogPrint("Document uploaded successfully");

}

function uploadDocumentnVerify(string[][] memory data,address[] memory studentAddressList,uint count) public { //only by university//

require(universities[msg.sender], "Only Registered university is allowed"); require(data.length >= count || studentAddressList.length >= count , "Count exceeds array

length");

require(data.length==studentAddressList.length,"elements mismatch"); for(uint i=0;i<count;i++){

require(data[i].length == 2, "Each data row should have 2 elements");

Document memory document = Document({ owner: studentAddressList[i], universityAddress: msg.sender,

ipfsHash: data[i][1], verified: true

});

function verifyCompany(address companyAddress) public onlyOwner{ require( !companies[companyAddress],"company alredy verified"); companies[companyAddress] = true;

emit LogPrint("company verified successfully");

}

Document storage document = documentsById[uniqueId];

require(document.owner!= address(0), "Document does not exist");

require(document.owner==msg.sender||document.universityAddress==msg.sender,"The user is not authorized to access document" );

mapping(address => bool) storage companiesm = AccessCompanyMapping[uniqueId]; uint256 count;

// First, count the number of addresses that have true values for (uint256 i = 0; i < companyAddresses.length; i++) {

if (companiesm[companyAddresses[i]]) { count++;

}

}

// Collect the addresses with true values

for (uint256 i = 0; i < companyAddresses.length; i++) { if (companiesm[companyAddresses[i]]) {

allowedCompanies[index] = companyAddresses[i]; index++;

}

}

return allowedCompanies;

}

function getDocumentDetails(string memory uniqueId) public view returns(string[2] memory,address[2] memory){

require(bytes(uniqueId).length > 0, "uniqueId cannot be empty");

Document storage document = documentsById[uniqueId]; require(document.owner!= address(0), "Document does not exist");

require(AccessCompanyMapping[uniqueId][msg.sender]

||document.owner==msg.sender||document.universityAddress==msg.sender,"This user is not

authorized to access document" );

string memory verifiedStr = document.verified ? "true" : "false";

return ([document.ipfsHash, verifiedStr],[document.owner,document.universityAddress]);

}

}

### IpfsConnect.jsx:

'localhost'; const ipfs\_port = 5001;

let ipfs;

// Function to initialize IPFS client async function initIPFSClient() {

try {

ipfs = create({

host: IPFS\_NODE\_HOST, protocol: "http",

port: ipfs\_port,

});

// Check IPFS connection status

const isOnline = await ipfs.isOnline(); if (isOnline) {

console.log("connected to IPFS");

} else {

console.log("IPFS client failed to connect");

// Handle connection failure here

}

} catch (error) {

if (error.code === "ECONNREFUSED") { console.error("IPFS server is not running or accessible");

// Handle connection refusal error here

} else {

console.error("Error connecting to IPFS server:", error);

// Handle other connection errors here

}

}

}

export {ipfs,initIPFSClient}

### Ipfsfn.jsx:

import { ipfs } from "./ipfsConnect.js"; import fs from "fs";

import { PDFDocument, rgb } from "pdf-lib"; import { v4 as uuid } from "uuid";

import path from "path"; import

QRCode from "qrcode";

import multer from "multer"; import express from "express"; const ipfsRouter = express.Router();

"./uploads"); const APPENDED\_DIR = path.join(process.cwd(), "./appended");

if (!fs.existsSync(UPLOADS\_DIR)) { fs.mkdirSync(UPLOADS\_DIR);

}

if (!fs.existsSync(APPENDED\_DIR)) { fs.mkdirSync(APPENDED\_DIR);

}

const upload = multer({

storage: multer.diskStorage({ destination: function (req, file, cb) {

cb(null, UPLOADS\_DIR);

},

filename: function (req, file, cb) {

const ext = path.extname(file.originalname); const id = uuid();

cb(null, id + ext);

},

}),

});

export {upload};

//////////////////////Setup END////////////////////////////

///////////////////IPFS\_UPLOAD\_FN////////////////////////////// async function uploadFileToIPFS(filePath) {

const file = fs.readFileSync(filePath); const result = await ipfs.add(file, {

pin: true,

});

return result.cid.toString();

}

/////////////////////////////////////////////////////////////

////////////////////////REQUEST////////////////////////////////////////

/// uploading fn//

ipfsRouter.post('/upload', upload.single("certificate"), catchAsync(async (req, res) => {

try {

if (!req.file) {

throw new createHttpError.BadRequest("file not found");

}

const id = uuid();

const cid = await uploadFileToIPFS(req.file.path);

res.json({

uuid: id,

ifpsLink: `http://localhost:8080/ipfs/${cid}`,

//`https://ipfs.io/ipfs/${cid}/?filename=${id}.pdf`, cid: cid.toString()

});

} catch (error) { console.error(error);

res.status(500).json(

{ error: 'An error occurred while uploading the file' });

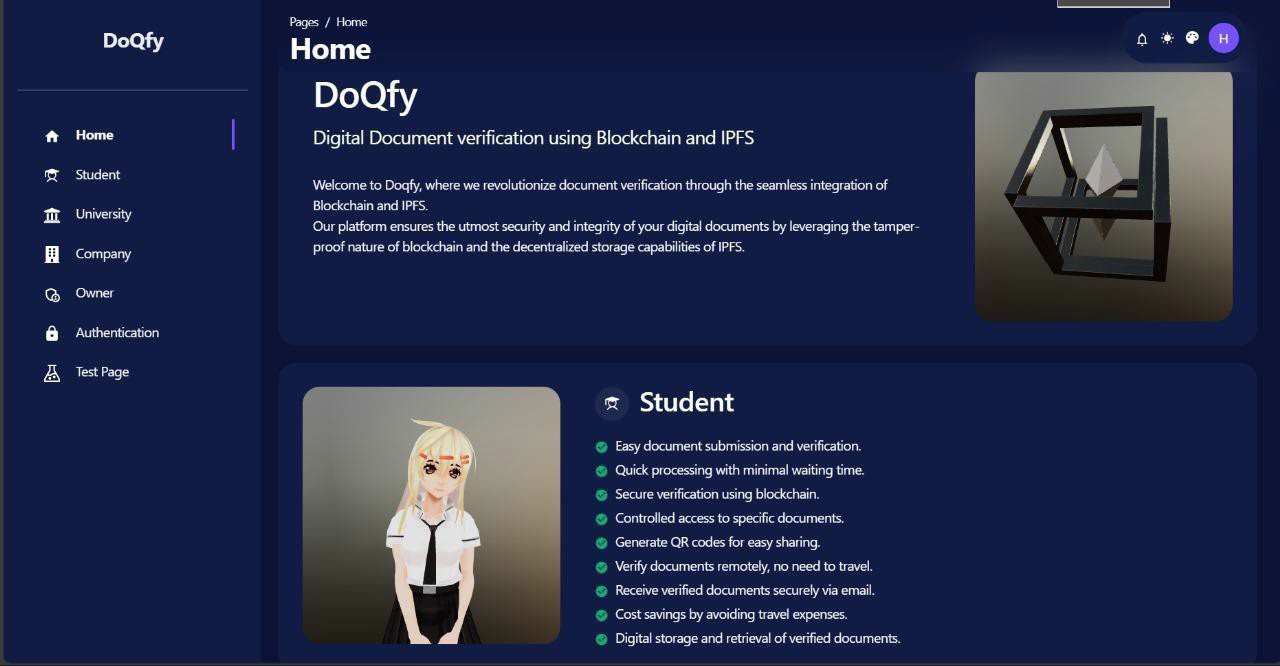
}

//issue//

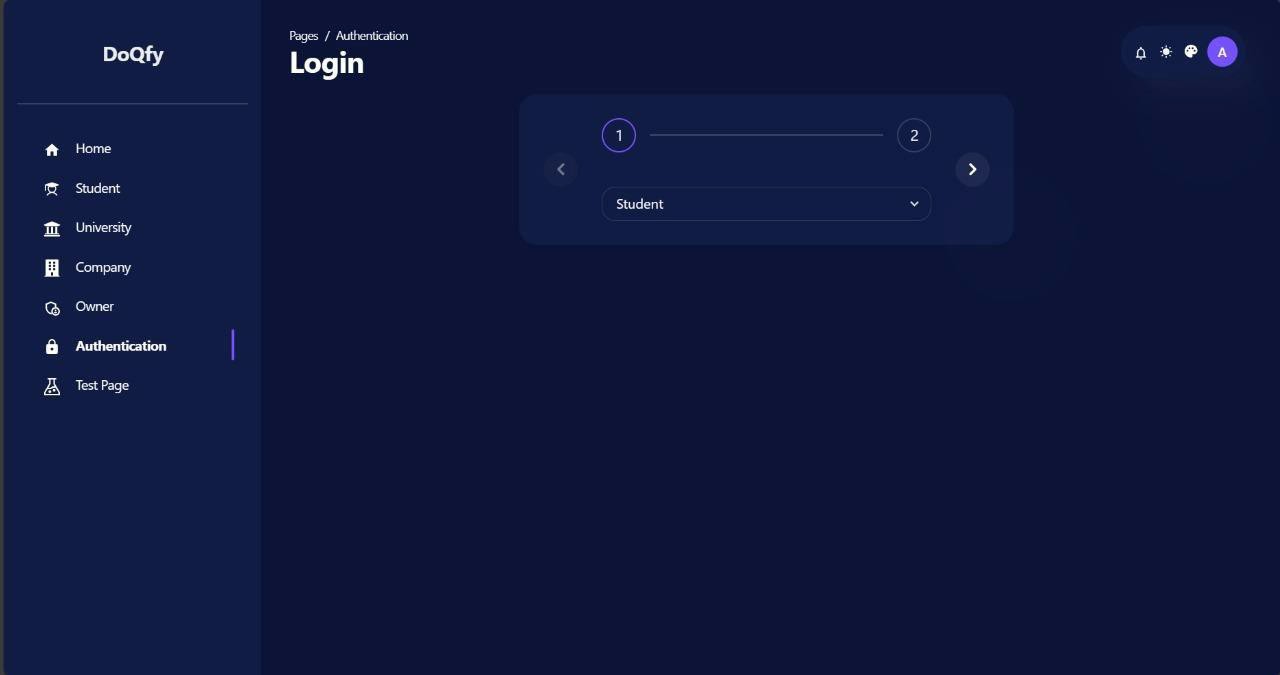
export default ipfsRouter;

# APPENDIX:2

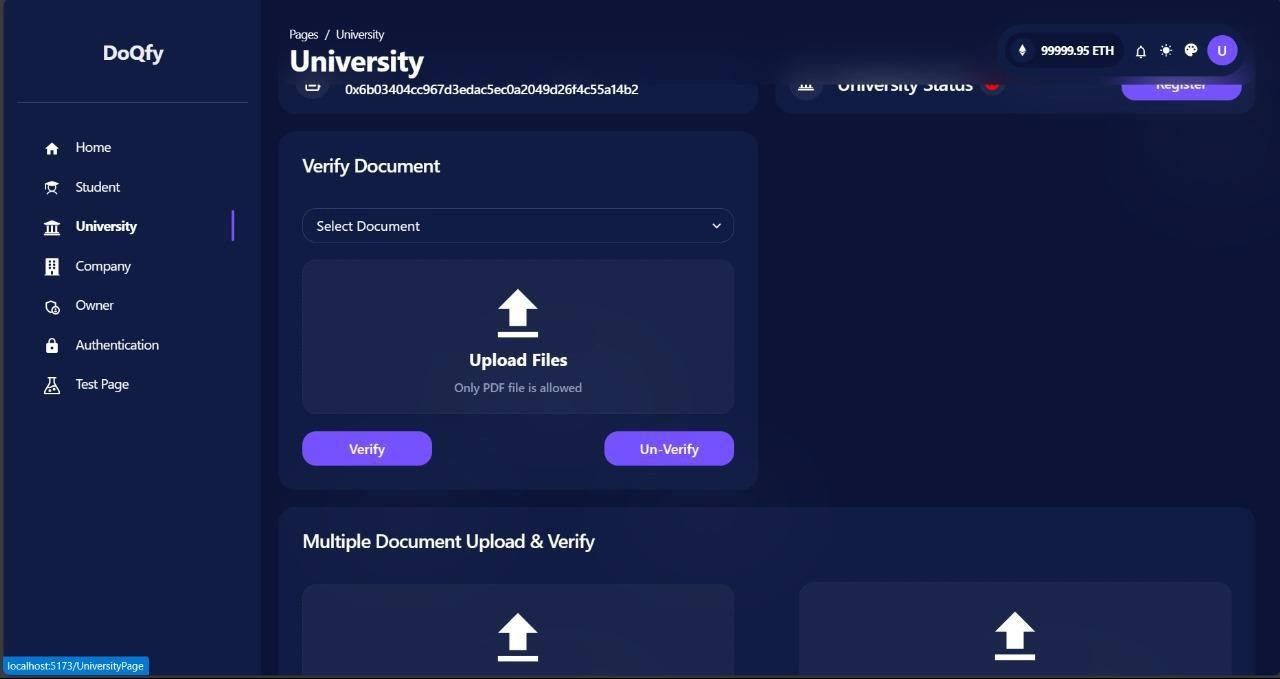
**SCREENSHOTS**



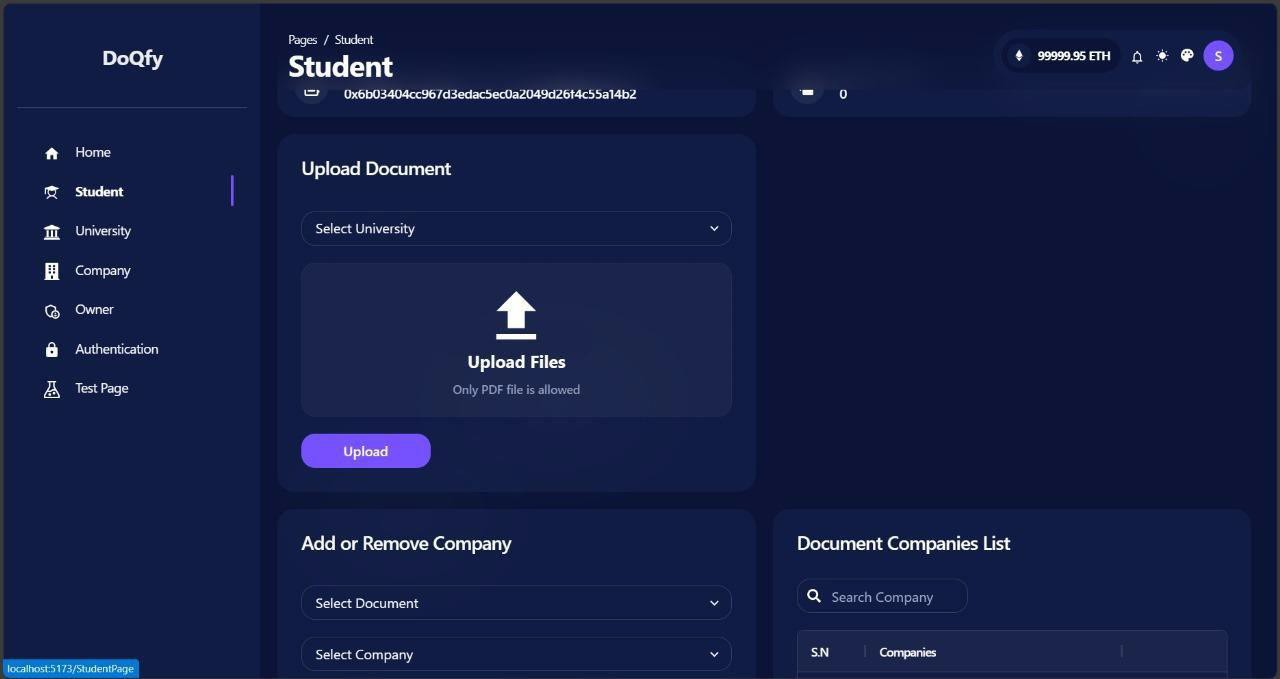
**Figure No A.2.1: Home Page**



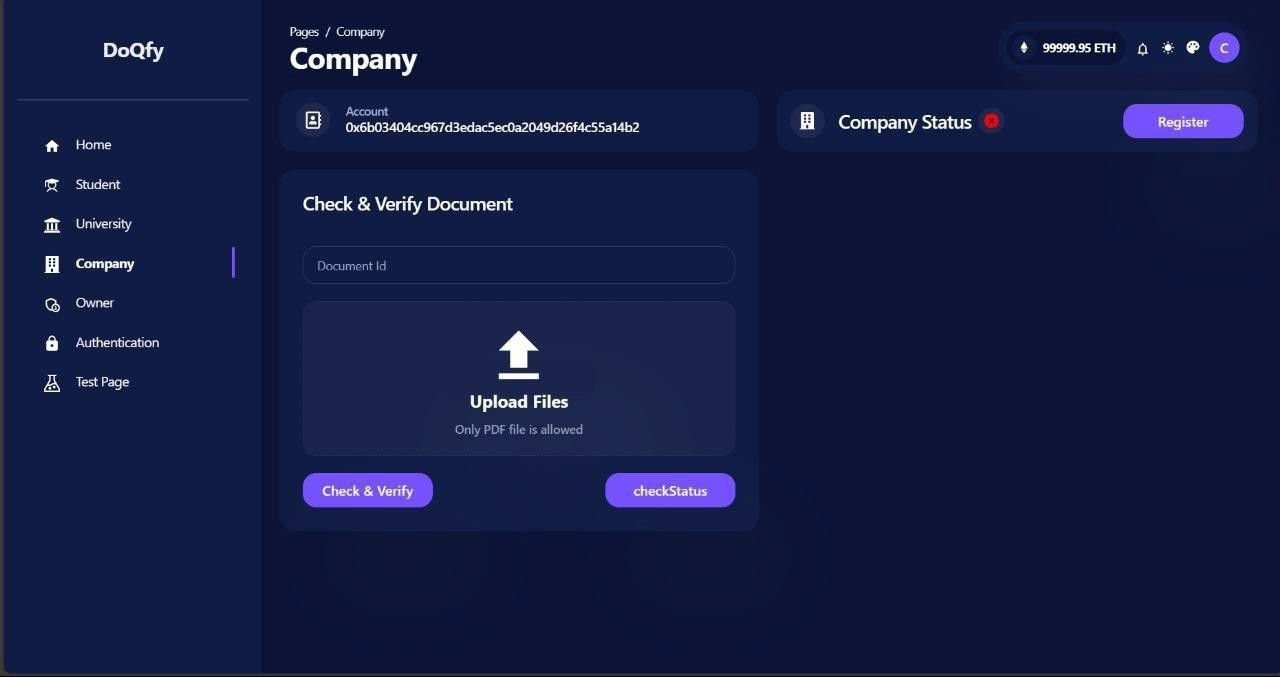
**Figure No A.2.2: Login Page**



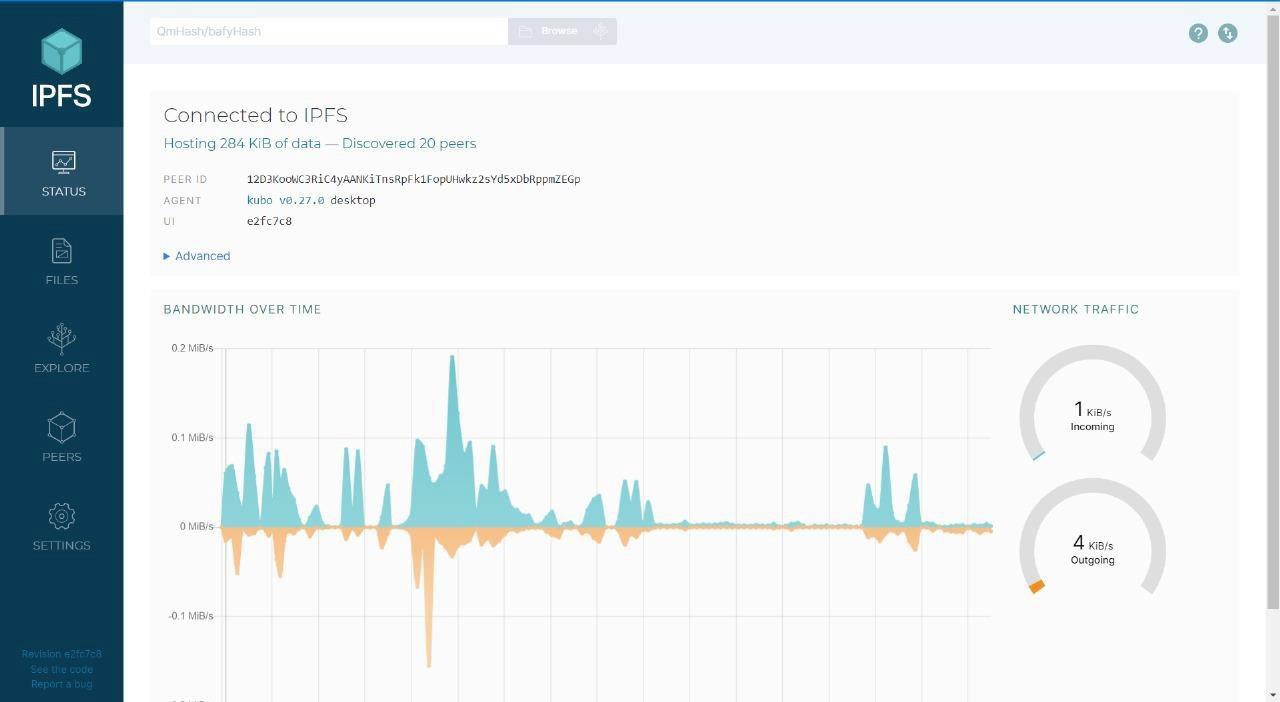
**Figure No A.2.3: University Page**



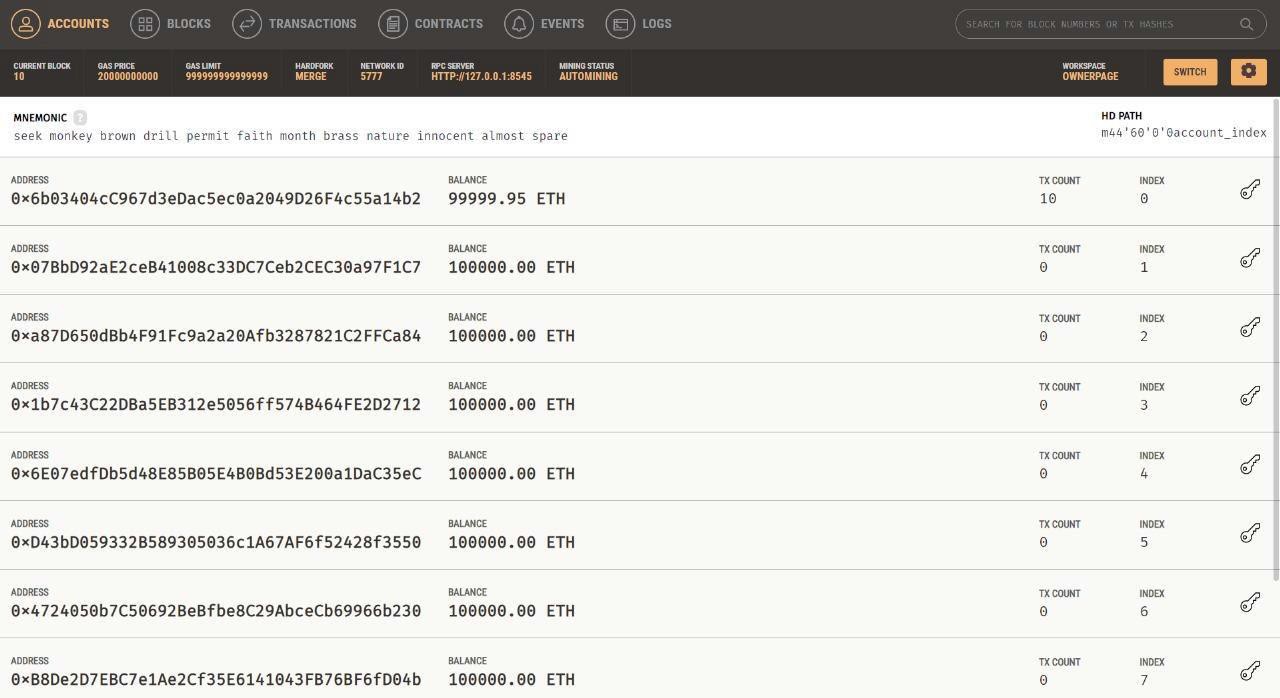
**Figure No A.2.4: Student Page**



**Fig No A.2.5: Company Page**



**Fig No A.2.6: IPFS Connect**



**Fig No A.2.6: Transaction page**

## REFERENCES

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf
2. Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform. Retrieved from https://ethereum.org/whitepaper/
3. Rosic, A. (2017). What is Blockchain Technology? A Step-by-Step Guide For Beginners. Retrieved from https://blockgeeks.com/guides/what-is-blockchain- technology/
4. Storonsky, S., & Simpson, I. (2018). Blockchain: Opportunities for Private Enterprises in Copyright Management. International Journal of Innovation Management, 22(1), 1850005.
5. Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.
6. Dimitrov, D. (2020). Blockchain-Based Solutions for Digital Copyright Management: A Systematic Review. Journal of Information Science Theory and Practice, 8(1), 28-49.
7. Haskel, J., & Westlake, S. (2017). Capitalism without Capital: The Rise of the Intangible Economy. Princeton University Press.
8. Larimer, D. (2016). Graphene: A Delegated Proof of Stake Consensus Algorithm. Retrieved from https://bitshares.org/technology/delegated-proof-of-stake- consensus/
9. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In IEEE International Congress on Big Data (pp. 557-564). IEEE.
10. Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin.
11. Kshetri, N. (2017). Will blockchain emerge as a tool to break the poverty chain in the Global South? Third World Quarterly, 38(8), 1710-1732.
12. Schueffel, P. (2016). Blockchain technology and the financial services market. SSRN Electronic Journal.









