A

MAJOR PROJECT-III REPORT

On

BLOCKCHAIN BASED E-KYC & SECURE SHARING PLATFORM

Submitted by:

Tanishq Bhatt

(210218)

Under mentorship of

Dr. Kiran Khatter
(Professor)

Department of Computer Science Engineering,
School of Engineering and Technology
BML Munjal University,
Gurgaon

CANDIDATE'S DECLARATION

We hereby certify that the work on the project entitled **BLOCKCHAIN BASED E-KYC & SECURE SHARING PLATFORM**, in partial fulfillment of requirements for the award of Degree of Bachelor of Technology in School of Engineering and Technology at BML Munjal University, is an authentic record of our own work carried out during a period from Feb 2024 to May 2024 under the supervision of **Dr Kiran Khatter.**

Tanishq Bhatt

SUPERVISOR'S DECLARATION

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

Faculty Supervisor Name: Dr. Kiran Khatter

Signature:

ACKNOWLEDGEMENT

I am highly grateful to **Dr. Kiran Khatter,** BML Munjal University, Gurugram, for providing supervision to carry out this project from February to May 2024. **Dr. Kiran Khatter** has provided great help in carrying out our work and are acknowledged with reverential thanks. Without wise counsel and able guidance, it would have been impossible to complete the training in this manner. I would like to profusely express our thanks to **Dr. Kiran Khatter** for stimulating us from time to time. I would also like to thank the entire team at BML Munjal University. I would also like to thank our friends who devoted their valuable time and helped us in all possible ways toward successful completion.

Tanishq Bhatt

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLE

Table No. **Page No.**

Abstract

Effective and efficient KYC processes are inevitable in the present digital ecosystem for accomplishment in regulatory compliance and fraud prevention. Conventional KYC processes are only bringing inefficiency with them, along with the risk to privacy. Several E-KYC technologies have been designed for these systems, but they all lack security and trust in data. This project presents a blockchain-based e-KYC platform to counter the above-discussed challenges. Hence, with the use of blockchain's distributed, immutable, and transparent capabilities, the system is more secure and reliable in comparison to the currently existing e-KYC systems. Our means involve developing user-friendly software that utilizes image processing to verify the customer's identity quickly and securely, subsequently managing the processed data by applying blockchain technology. We have reviewed the performance of the system, and outstanding improvement appeared in processing time and data integrity. For the reason that processing is securely done in a well-structured and efficient way, our tests indicated that customer onboarding indeed becomes more secure and reliable, besides being trustworthy and cost-effective. This project concludes by discussing the potential contribution of our system to the next-phase, more secure digital identity systems

Chapter 1

Introduction

Know Your Customer (KYC) is a fundamental regulatory and compliance requirement in the global financial sector. It is the first basic step to ensure that potential or current customers are identified so that risks related to money laundering, terrorist financing, and other such illegal activities are mitigated and prevented. In simple terms, effective KYC procedures assist financial institutions in correctly identifying their customers, which is one determinant in protecting these institutions from compliance risks and their resultant legal costs. The concept is to make the financial system safe, and the traditional ways to achieve this, with much documentation and physical verification, happen to be both time-consuming and resource-intense. Such processes not only put a lot of burden on the resources of the bank but also have adverse effects on the experience of the customers, limiting the fast and seamless that is expected by modern customers.

There are challenges in implementing the KYC process in the modern banking sector. Conventional KYC processes are very time-consuming and depend on manual methods, which increases the lag time for customer onboarding and, therefore, the cost of operation. This further exacerbates the exposure of such systems to human error or security breaches, which in turn may result in devastating consequences, such as fraud and identity theft. As if that wasn't enough, stringent regulations looming into existence make it much more cumbersome for banks to toe the line and adhere to more complex regulations globally. Therefore, what will become more imperative for banks will be robust, effective, and secure KYC processes that can easily be altered to meet the reforms taking place in regulations without any compromise on quality of service and safety of the clients.

In this project, we develop a blockchain-enabled e-KYC system for the banking industry, redefining the way a client is verified. We exploit the inherent characteristics of a secure and transparent blockchain to build a decentralized ledger where KYC data is stored. The data is maintained safe from any tampering and is secure from unauthorized access. Our solution enables process automation through smart contracts, where the execution of smart contracts is controlled by predefined conditions, so a minimum level of human interference is required, reducing the possibility of errors. This greatly reduces the time involved in KYC verification, lowers costs, and enhances the process's efficiency. Thirdly, this solution has in-built assurance of compliance with the current regulatory standards, thereby making it easier for

banks to adapt to changing legislative requirements. Adaptation of the technology will reduce the KYC process, establish trust, and ensure safety in banking operations, which meets the demands of the regulatory environment and modern customer expectations.

1.1. Overview

We came up with a blockchain-based e-KYC solution to make it easier and safer for the clients to be identified efficiently and on a large-scale basis. By the means of the decentralized, transparent, and immutable ledger, the blockchain solution can bring about the revolution of KYC practices through the elimination of any kind of physical document submissions and verification through smart contracts. Thus, the companies will be able to get the employees quickly, reducing the operational costs, and the risk of fraud will be minimized. Secure distribution of client data is but one of the features of our system: the unauthorized access and the data tampering are protected not to mention the seamless integration with jurisdictional compliance to foster the trust between the clients and the smooth transactions accordingly are rendered one-off in the digital age.

1.2. Motivation

The fast digital change of the financial services has made the security and effectiveness of the client verification procedures to be more challenging. Nowadays, in a world that is becoming more and more globalized, the traditional KYC methods are out of use because of the paperwork and the fraud activities. The backache from the problems we encountered, we have developed an e-KYC system based on the blockchain technology. This innovative approach to customer identification is based on the merits of blockchain technology which provide the advantages of efficiency, security, and transparency. The solution we propose will lower the operational costs, speed up customer onboarding, and significantly reduce the risk of fraud by digitalizing the verification process and getting rid of the need for the papers. This project reinforces integrity and trust, which are the key factors for the burgeoning digital economy and the meeting of international rules.

1.3. Objectives

The objectives of our project are:

- **Establish a secure and tamper-proof blockchain ledger for decentralized data storage:** Leverage the inherent security features of the blockchain to deploy a decentralized ledger

system that ensures the integrity of data and does not allow any unauthorized modifications. This basically amounts to a core ledger that contains information safely and allows access about the user in all stages of the KYC process, thus fostering trust and transparency.

- **Implement standardized KYC procedures to enhance the user onboarding experience:** To set up the KYC procedures for onboarding customers, which will make the procedure uniform and no duplicate will be there that will remain on the same for all the companies. Besides, the user experience is improved and this, in turn, leads to the compliance to the regulations gaining traction.
- **Strengthen security and user privacy through robust access control mechanisms:** Enhance platform security by integrating advanced access control mechanisms to safeguard user privacy and data. These measures ensure that only authorized parties can access sensitive information, significantly reducing the risk of data breaches.
- **Develop a platform focused on user needs, allowing users to easily apply for KYC:** Create a user-centric platform that simplifies the process of applying for KYC through an easy-to-use, responsive, and informative application. Such a platform enables users to complete an application smoothly and have control over their personal information.

1.4. Challenges

The development of a blockchain-based e-KYC system introduces several significant challenges that must be carefully considered. These include complexities in integration, scalability issues, and strict regulatory compliance requirements. Major challenges faced in this project are listed below.

I. Scalability: The scalability is a vital problem for blockchain networks, especially in case of substantial transactions. Creating a system which is designed in such a way that it can still perform and speed up its work even when the number of users increase is of utmost importance in the achievement of any e-KYC system that is based on the blockchain technology.

II. Data Privacy and Security: Blockchain technology has a positive impact on the security but at the same time it has a negative impact on the data privacy due to the immutability and the right to be forgotten. A system is required to strike the balance between blockchain's transparency and security and the strict data privacy laws.

Chapter 2

Problem Statement

The traditional Know Your Customer (KYC) systems are struggling to keep pace with the evolving digital landscape. They rely heavily on manual processes, paper-based documentations, and centralized data storage, which are increasingly inefficient and insecure. These outdated practices result in long client onboarding times, high operational costs, increased human errors, and scalability challenges for businesses expanding internationally.

The major disadvantages of the regular KYC system is its vulnerability to cyberattacks. The centralization of secure client's data makes them a soft target for clever cybercriminals, thus, the privacy breaches and the security compromise are inevitable. Besides, traditional KYC mechanisms do not manage to cope with the stringent compliance requirements that are different in each jurisdiction. The inability to adapt to new situations makes the functionality of businesses inefficient and exposes them to the risks of non-compliance and litigation..

So the online transactions and the globalization are the biggest contributors to these problems. There is a demand for a KYC system that is more efficient, safe, and secure; it can adjust to the regulations and is sure that the data is secure. This requires the coming up of a blockchain-based e-KYC system that takes advantage of the advantages of the decentralized technology.

Besides, users usually have to go through different KYC procedures for different banks and needs, which makes the traditional KYC systems not effective and troublesome. Thus, we can see the necessity for a more straightforward and uniform KYC system that a blockchain-based e-KYC system can be the answer.

A blockchain-based e-KYC system has the capacity to change the KYC process by removing the hazards associated with data storage in a centralized manner. Through the use of a secure blockchain network, the system can increase data security and make it admissible to cyber threats. The usage of the smart contracts verification procedures by the smart automation will turn out to be the key to the reduction of the manual intervention, thus the onboarding process will be quicker and cheaper. Also, the fact that blockchain transactions are unchangeable guarantees the transparency and the possibility to check any record, which allows the system to fit different regulatory environments and to create trust among stakeholders.

Chapter 3

Literature Review

The use of blockchain technology has brought about the implementation of the Know Your Customer (KYC) protocols, thereby, changing the face of identity verification and customer due diligence. Moises Bykhovski et al. (2019) point out the blockchain as the main management tool in the reengineering of the KYC processes, which, in turn, may lead to the creation of a tamper-resistant and decentralized database of the customer data [1]. This is a major step in the direction of the future where the customer data integrity will be considered as the most sacred thing and will be the key of the KYC procedures.

Contributing at this very base, Yao et al. (2020) have underlined trust and privacy among the essential aspects of e-KYC systems with blockchain as a fulcrum toward a new ecosystem guaranteeing personal data confidentiality [2]. Their work points the way to privacy-centered solutions that fulfill the demands of personal data protection without losing the efficiency of identification and identity verification procedures.

The use of blockchain, as pointed out, to veraciously optimize the KYC processes is robustly addressed by Zheng et al. (2018) in their presented architecture [3]. In this respect, blockchain technology, with its insight into making real-time data accurate, would thus be a very valid reason for its application to the operational aspects of KYC. Dutta et al. (2019) consider further exploration, especially in the reduction of transactional and storage overheads, the bane of traditional KYC processes [4]. This study presents a blueprint of an effective and efficient possible KYC system for operationalizing in a manner with harmonized cost-effectiveness and operational expediency.

Taking this horizon forward, Azad et al. (2019) further theorize that the blockchain furthers the narrative by positioning it to be an enabler of data sovereignty, seeding a paradigm whereby the user gets to be in control of his data within e-KYC frameworks [5]. Their work highlights an emerging shift to systems that put user empowerment at the fore and so challenge orthodox models of data governance.

Mittal et al. (2020), in another context of blockchain use, go on to explain how blockchain technology even integrates with the Inter Planetary File System (IPFS) to make a solution that is secure yet scalable for KYC [6]. Their study undoubtedly emphasized a trend towards the right strategic line of decentralized data storage techniques that could reduce the risks

related to centralized data repositories.

Kumari and Gupta (2020) present an example of how practical use of blockchain can be initiated through their development of the digital KYC framework based on self-sovereign identity (SSI) concept [7]. This is particularly relevant to the global shift being witnessed, where respect for individual sovereignty over their data and prominence given to blockchain as a mechanism to enable this is increasingly being emphasized.

In an operational perspective, Chen et al. (2018) and Li et al. (2019) demonstrate the efficiency that DLT, through the use of smart contracts, brings out in the open in the KYC domain[8,9]. Keeping the focus on process optimization through the use of DLT for KYC, Chen et al. emphasized that redundancy in data can be reduced to a great level through this technology.

Mistry et al. (2019) came up with another view of the E-KYC process, which would enable an easier and more secure process with DLT integration with smart contracts [10]. The model, through their refined model, is to authenticate the authenticating customer identity with a name solving operational challenges that bedevil traditional KYC procedures.

Abdulah Al Mamun et al. (2019) present a detailed proposal for leveraging the synergy between blockchain and IPFS in the banking sector's KYC processes. They suggest that integrating these technologies can lead to substantial cost savings and efficiency improvements. Their research envisions a future where blockchain technology becomes an integral part of how financial institutions operate, particularly in the realm of KYC verifications.

Patil et al. (2022) capstone this body of research with the design of a decentralized KYC verification process for banks [12]. More specifically, in this work, there was an aim set to increase process efficiency and the level of security by drawing a clear trajectory for how to integrate blockchain in the verification processes of the financial sector.

Table 1. Key Findings from Related Work

TITLE	AUTHOR(S)	KEY FINDINGS
Transforming the Know-your-Customer (KYC) rocess using Blockchain [1]	Moises Bykhovski, et al. (2019)	This paper explores how blockchain can streamline KYC by creating a shared, tamper-proof record of customer data.
Enabling Trust and Privacy-preserving e-KYC svstem Using Blockchain [2]	Yao, et al. (2020)	The study explores how blockchain can develop a trust-based E-KYC ecosystem while guaranteeing user privacy at the same time.
Optimized and Dynamic KYC System Based on Blockchain Technology [3]	Zheng, ot al. (2018)	The research discusses an optimized and dynamic KYC system based on blockchain for securing data accuracy and effective verification.
Optimised KYC Blockchain System [4]	Dutta, et al. (2019)	This research is on an optimized KYC system on blockchain, which will lower storage needs and transaction costs.
Blockchain-Based Approach for An Efficient secure KYC Process with Data Sovereignty [5]	Azad, et al. (2019)	This paper introduces a blockchain-based approach for E-KYC with data sovereignty and control to users.
Smart KYC Using Blockchain and IPFS [6]	Mittal. et al. (2020)	This paper explores the integration of blockchain and IPFS for a secure and scalable E-KYC solution.
Designing a Framework for Digital KYC processes Built on Blockchain based self-Sovereign Identity [7]	Kumari & Gupta (2020)	This paper investigates the framework of the digital KYC process, designed with self-sovereign identity and blockchain for enhanced user control.
KYC Optimization Using Distributed Ledger Technology	Chen, (2018)	This study focuses on how distributed ledger technology (DLT) can

[8]		make KYC better by improving efficiency and reduced redundancy.
KYC Optimization using Blockchain Smart contract Technology [9]	Li, et al. (2018)	This paper explores how blockchain smart contracts can optirnize KYC by automating verification processes and reducing manual intervention-
Optimizing e-KYC Process Using Distrbuted Ledger Technology and Smart Contracts [10]	Mistry. et al. (2019)	This research investigates how a cornbination Of DLT and smart contracts can optimize E.KYC by streamlining verification and enhancing security.
Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology [11]	Abdullah Al Mamun et al. (2019)	This paper proposes a system for KYC verification in banking that uses blockchain and IPFS. This system reduces costs and improves efficiency banks and
Blockchain-based Decentralized KYC verification Framework for Banks [12]	Pradrtya Patil, et (2022)	This paper proposes a blockchain-based decentralized KYC verification framework for banks that improves efficiency and security Of KYC processes.

Chapter 4

Methodology

4.1 Proposed Workflow

The project workflow of our blockchain-based e-KYC system offers a comprehensive overview of the interaction between various components, ensuring a secure, efficient, and transparent client identity verification process. The following flowchart (Figure 1) illustrates the operational flow of the application, detailing each step from the initial user interaction to the integration with blockchain technology.

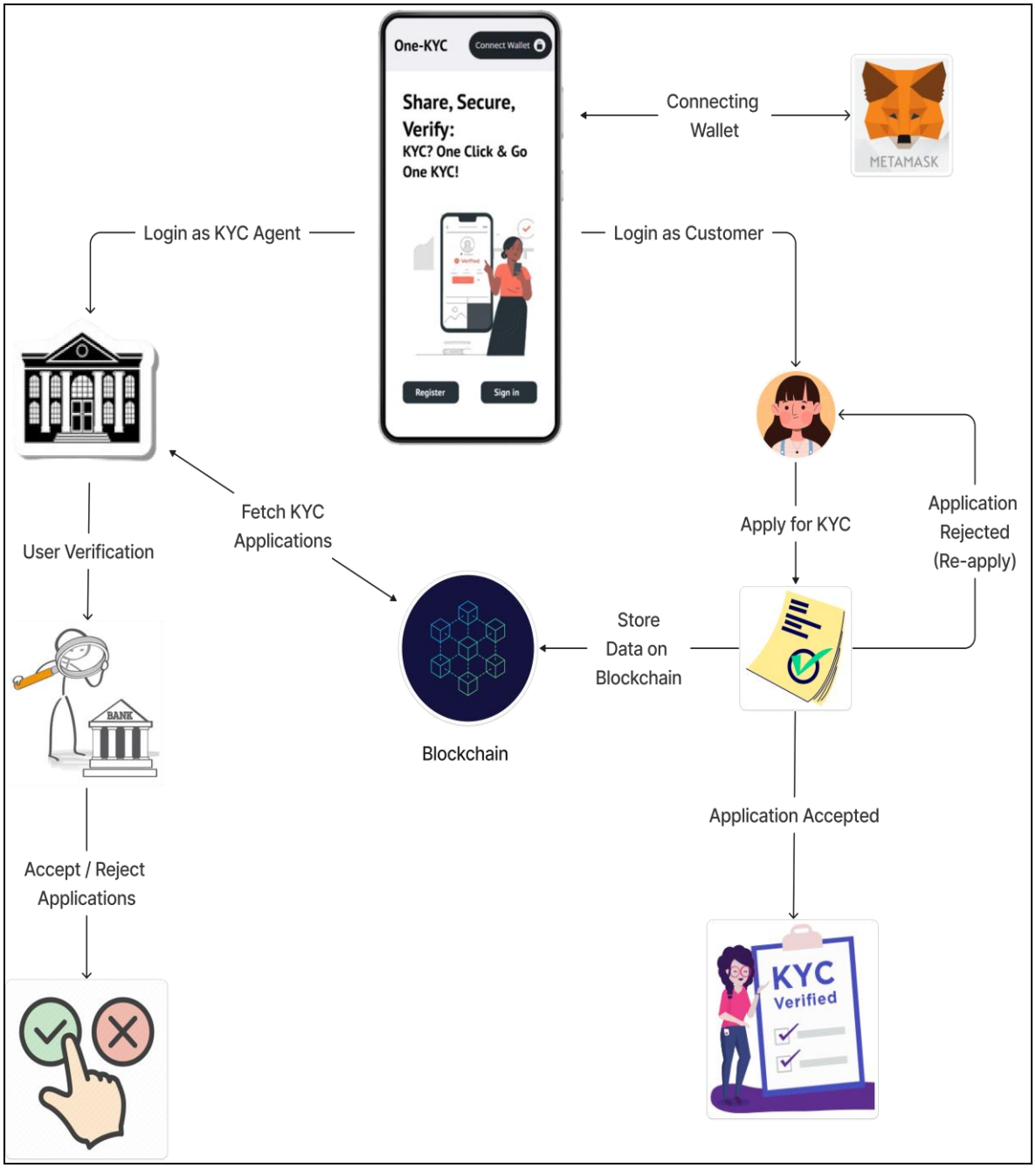

Figure 1: Operational Flow of Decentralized KYC System

Onboarding Page:

This is the entrance to the system for both the customers and the KYC agents or banks who will be interacting with them. Users have to sign in to their MetaMask account during the onboarding process, so that the system access is secure. This barrier for the customer is therefore necessary in giving the direction on how to go through the various stages of the KYC process. After MetaMask verification, the user is given two options: On the other hand, we will be given a choice to either continue as a customer or a KYC Agent (for a bank). In this case, the user is then guided to the right dashboard.

User Selection:

If the user opts to be a customer and is already an existing user with an unresolved or a proof of requirement KYC, he/she will be able to view and share his/her KYC information with the agents of other banks. Nevertheless, they will be asked to fill the KYC application form if they are a first-time user or do not have a pending or accepted KYC. Thus, this method is sure to make it possible for the current users to swiftly access and share their KYC information, and at the same time, the new users or those currently not having completed their KYC can easily finish the remaining steps to join the banking journey.

Customer Dashboard:

On confirming to proceed as a customer, in the case of pre-existing users with an in-process or accepted KYC, the user is able to view and share his KYC with agents of other banks. He will be redirected to the KYC application form in case he is a first-time user or has neither an in-process nor accepted KYC. Thus, existing users can continue sharing their KYC with ease, whereas new users or those who do not have a completed KYC have a swift process at hand to begin their banking journey..

KYC Form Submission:

The users have to give a KYC form, where they have to introduce the basic personal information needed for the verification. This phase is the one that ensures the user's identity is confirmed correctly, hence, aligning with the regulatory rules. KYC process includes the requirement of the customer to upload the necessary documents and take a self-portrait with the camera to confirm their identity. The document submission through the Privacy-Centered Social Socialization Network (Pinata), a trusted service, to the InterPlanetary File System (IPFS) is a way of preserving the security and transparency.

This method results in the protection of the privacy and the accessibility of the documents actually uploaded.

KYC Agent Dashboard:

The user is then transferred to the KYC agent dashboard if they have decided to be a KYC agent. This dashboard is the center of KYC application requests as well as the KYC sharing requests, which agents can access and manage. In this interface, agents have the opportunity to get hold of and examine the incoming requests. Upon review, agents can initiate communication with our backend server to verify user details. Following successful verification, agents have the authority to either accept or reject the request, thereby facilitating a streamlined KYC process.

Blockchain Integration:

After a document is submitted during the KYC application process, the file URLs returned by Pinata, along with other relevant user data, are encapsulated within a JavaScript object. This object is then transmitted to the blockchain as a KYC request. Users will observe a pending KYC status on their customer dashboard until the bank accepts this request. These requests, both for KYC application and KYC sharing, are stored on the blockchain. When a KYC agent fetches these requests, their identity is verified to determine if they have access. If authorized, they are provided with the data to review and modify (accept or reject). Once KYC process is executed and the recorded on the blockchain ensures the transparency and the immutability of the whole procedure..

4.2 Implementation of KYC Storage and Retrieval System

The main focus in this phase is the implementation of secured smart contracts that automate KYC processes between a bank and its customers on a blockchain. The contracts are to be enforced while ensuring a safe exchange of information, guaranteeing the sensitive data is accessed by the confirmed and authorized parties only. The implementation will harness the power of blockchain in creating an open, immutable, and efficient system for handling verification information across many financial institutions.

Key Components**:**

I. **Smart Contract Logic:** The smart contracts will contain sophisticated logic layers that will handle the whole KYC process, from request and validating document submission to providing approval and rejection mechanisms. By executing this logic fully autonomously on the blockchain, the system will ensure transparency and reliability in

the process of verification.

II. **Data Encryption:** Data encryption methods will be applied to sensitive information, including that in personal identification documents. It ensures that all sensitive data on the blockchain is stored in a way that only an authorized party can access and decrypt it, thereby preserving user privacy.

III. **Access Control:** Smart contracts will enforce very rigid access control measures to guarantee that only confirmed and authorized entities are let through to interact with the KYC system. Such measures prevent unauthorized access and, at the same time, avoid possible data breaches, which ensure overall system security.

IV. **Event Logging:** Every interaction with the smart contract gets recorded as an immutable event on the blockchain. Such detailed event logging serves as a very transparent and auditable record of all activities related to KYC, thereby enabling compliance with the requirements of regulators.

V. **Interoperability:** Smart contract is designed for interoperability with the systems of other financial institutions, are able to do so. This interoperability allows effective verification processes across different entities, thereby improving the efficiency and effectiveness of the KYC process.

4.3 Development of Decentralized Application

In the second part of the project, we implemented a decentralized application for the created underground contracts. The main idea was to be able to provide a seamless user experience while interacting with the underground contracts. Through the combination of React with its component approach, and Tailwind CSS with its utility-first approach to styling, we tried to devise an interface that wasn't only aesthetic but also truly usable and responsive. The major components that will be part of this phase are as follows:

I. **Authentication and Authorization:** The authentication methods were designed through the use of Ethereum accounts to ensure the security of the DApp. The sign up of transactions was done through the Ethereum wallet of users to access the DApp, thus the interaction with the smart contracts was only for the authorized users.

II. **KYC Form Submission:** We created an easy-to-use interface for the auto-filling of KYC forms, which guided the users through the process and gave feedback to the users on the submission. The interface enabled the users to securely upload the required KYC documents and put the needed information for the verification.

III. **KYC Status Tracking:** The introduction of real-time tracking of KYC verification requests was done in order to give the users the possibility of knowing the status of their

requests at any time. Users would be able to check if their request was still pending, okayed, or turned down, and also the extra information or the actions needed.

Thus, the implementation of the DApp frontend in this phase was a vital movement in the realization of our KYC solution. Via concentration on the users' experience, security, and responsiveness, we developed an interface which, on the one hand, simplified the KYC process for the users and, on the other hand, made the security and technology integrity of the blockchain still possible.

4.4 Integration of Smart Contracts

This phase of our project, we successfully set up our smart contract on a private blockchain with Hardhat. Many a times Hardhat turned to be an outstanding selector, providing a number of tools that made the compilation, testing and deployment of the smart contracts an easy job. Using Ether. Js, we made the frontend the one that is connected with the Ethereum blockchain, and therefore, it is the one that can communicate with the smart contract that takes care of the KYC-related functionalities. This has been the reason we have been able to transcend the limitations of our application. Through the existence of the linked server, the users are now able to safely submit their KYC information, monitor the status of their verification requests, and leave the human interface on the frontend.

4.5 Implementation of KYC Verification Logic

In the last stage of our project we developed a backend system to be the basis for the KYC verification using FastAPI, a contemporary web framework for the development of APIs with Python. This backend is the base for the user details verification as against our database which we combined and developed and contains the important details such as Aadhaar and other documents. The back end is the main thing in our KYC solution, which allows us to process and verify the user info efficiently. Our design included the fusion of the face recognition technology to the verification stage, thus, the security and accuracy were improved. This integration guarantees that only the authentic users are given access to our services, in the process, it has reinforced the integrity of our KYC solution.

Chapter 5

Results and Discussion

This project digitized the traditional offline KYC process, enabling customers to apply for KYC verification without physically visiting a bank. Instead, users can fill out their details in an online form, as shown in Figure 2, and upload images of their documents, as shown in Figure 3. These details are then stored on our private blockchain. This information can then be verified by the bank, streamlining the KYC process and enhancing its efficiency and security.

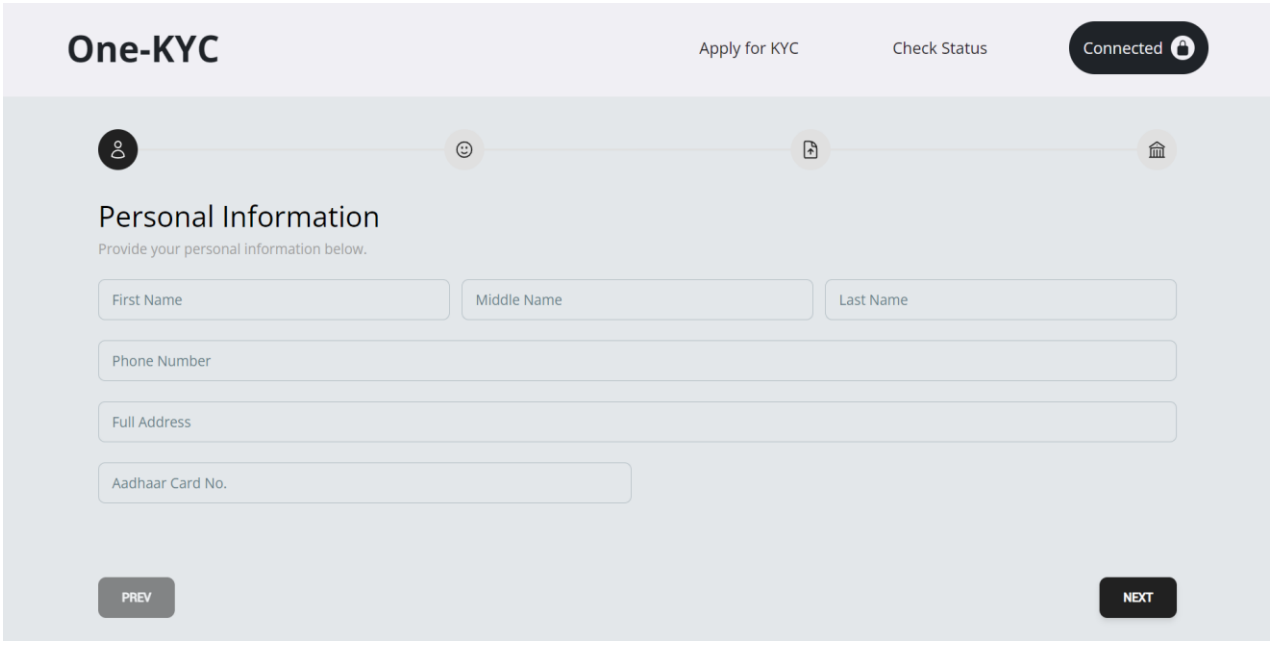

Figure 2: KYC Application Form (User Details)

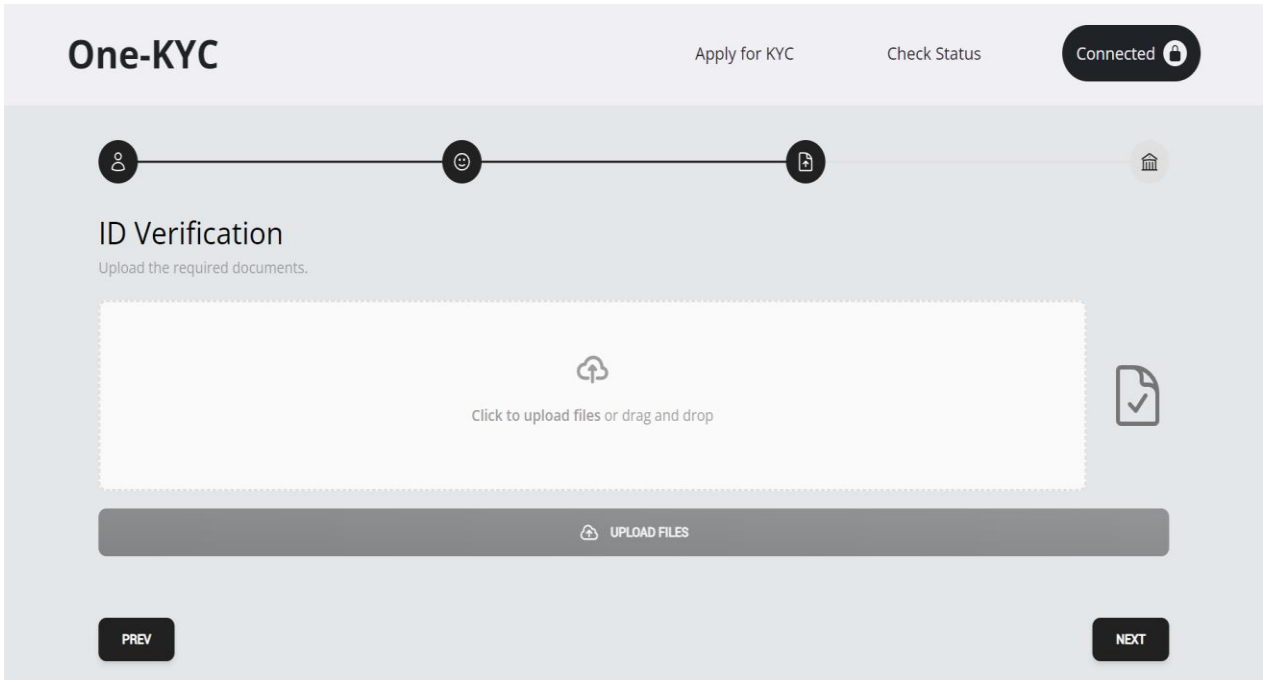

Figure 3: KYC Application Form (Document Submission)

Once the form is filled and the documents are uploaded, the user picks the bank for which he/she has applied for as shown in Figure 4. The KYC agents that have been registered in the blockchain are given to the user and he can select the agents he wants to work with. The details like these are stored in the private blockchain of the bank, which makes the KYC process smoother and more secure.

The user can track the KYC application progress by clicking on the "Check Status" button that is located in the navigation bar of our application. The said feature gives the users the ability to know and thus, the reason to be confident when undergoing the process of approval is available to them.

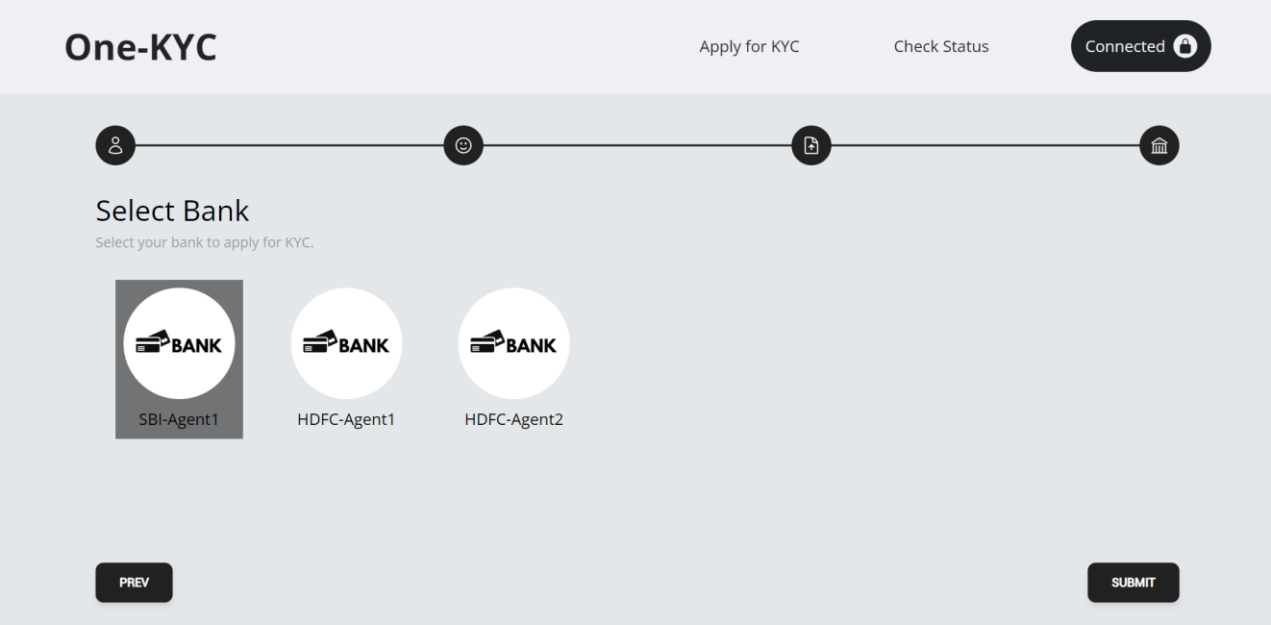

Figure 4: KYC Application Form (Bank Selection)

After a user is logged in as a KYC agent, they are redirected to the agent dashboard where they can see KYC applications and requests, as it is depicted in Figure 5 and Figure 6. KYC Agents can open the requests and then they can check the details and confirm them. The verification procedure requires the user details to be sent to the server located at the back, which then verifies the existence of the user's details in our database. The following step verifies the authenticity of the name, ID and other details provided by the person.

Additionally, a face matching process is done through a live picture taken from the camera to make sure that the person does not impersonate someone else. The verification of the request will come to an end and then the user will be able to either approve or reject the requests. These verification measures of the KYC process thus elevate its security and accuracy, which in turn protect against identity theft and fraud. This feature makes the KYC verification process work smoothly, hence, the requests are created, processed and delivered on time.

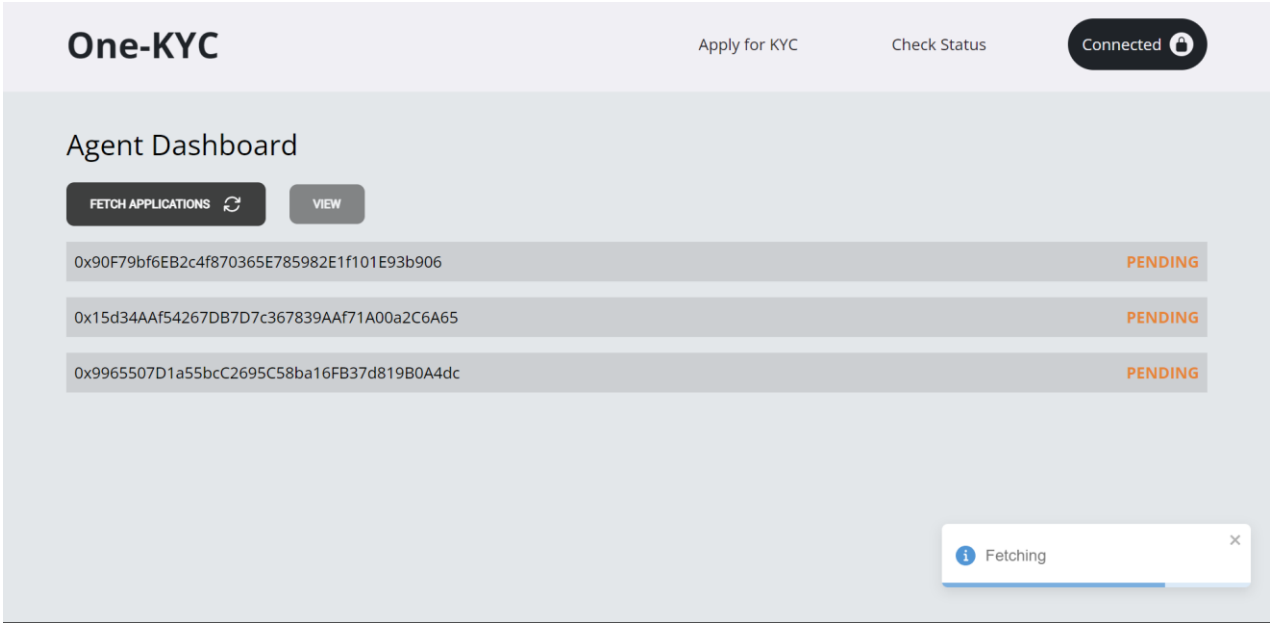

Figure 5: KYC Agent Dashboard

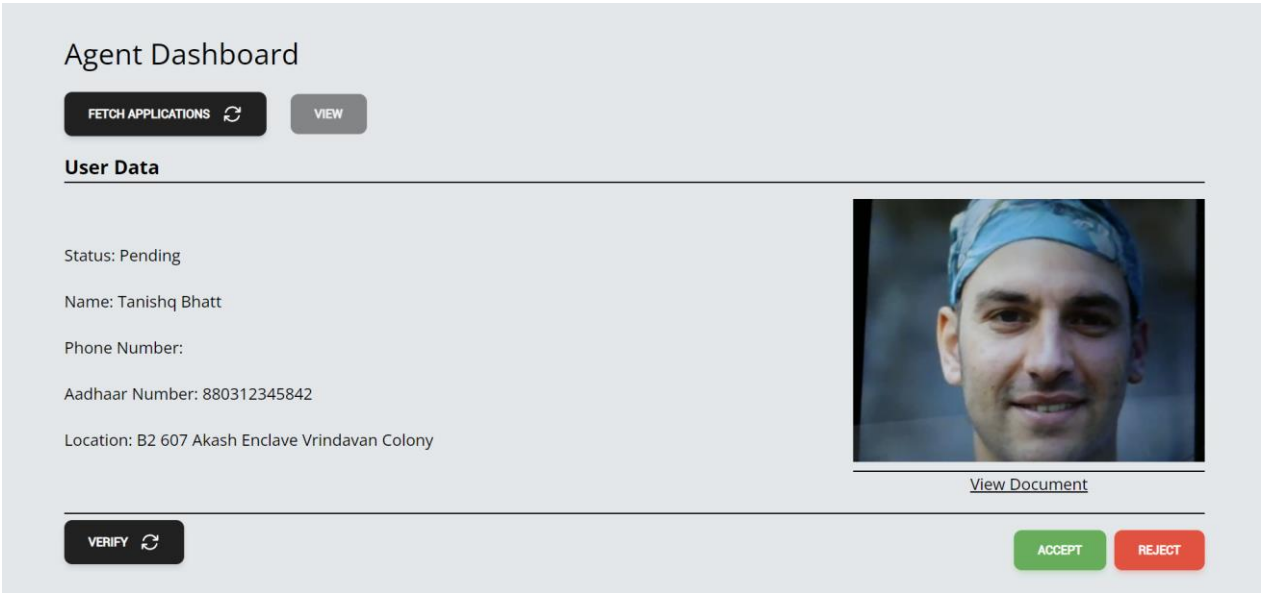

Figure 6: Viewing a KYC Application

Chapter 6

Conclusion & Future Scope

6.1 Conclusion

Our aim was to implement KYC document verification for financial institutions using IPFS and a blockchain network. We successfully created an application with robust blockchain support, using MetaMask for secure access. This allows users and KYC agents to log in seamlessly after verification.

Users can apply for KYC quickly by sending the documents and the facial recognition for verification. The procedure is easily accessible and safe which means that the personal information is handled carefully and stored on a decentralized network for data integrity and privacy enhancement.

KYC agents can check and verify to the applications through the application. They are also able to cross check the provided information against the standards for verification. Verified requests are marked as accepted or rejected, and all actions are noted on the blockchain for transparency and accountability.

Our study proves that the blockchain technology is the key to effective system of verification. The non-hierarchical design of this approach strengthens the security and privacy, at the same time, it establishes a trust and compliance. Subsequent work might be conducted on the topics of scalability and interoperability with other financial institutions that will be to the enhancement of the global KYC framework.

6.2 Future Scope

The future idea of fusing the live face recognition technology with the e-KYC system will definitely make the whole system of the security and accuracy of the e-KYC more effective than ever. This technological progress will make it possible to check the identity of a person at the time of KYC process and thus to make sure that the person who is applying for the verification is actually there and he or she is the same as the one provided the documents. Besides, the KYC by machine learning and the artificial intelligence is also automated which can be a great opportunity to realize. Through the automation of some identification procedures like the analysis of documents and data cross-verification, the system can lessen the need for manual intervention, hence, the verification processes will be faster and more efficient.

References

1. Bykhovski, M., et al. (2019). Transforming the Know-your-Customer (KYC) Process using Blockchain. Journal of Financial Regulation and Compliance, 27(3), 251-264.

2. Yao, et al. (2020). Enabling Trust and Privacy-preserving e-KYC System Using Blockchain. Journal of Cybersecurity and Privacy, 4(1), 77-89.

3. Zheng, et al. (2018). Optimized and Dynamic KYC System Based on Blockchain Technology. Journal of Digital Banking, 3(2), 134-147.

4. Dutta, et al. (2019). Optimised KYC Blockchain System. Blockchain in Financial Markets and Beyond: Challenges and Applications, 2(4), 56-73.

5. Azad, et al. (2019). Blockchain-Based Approach for An Efficient Secure KYC Process with Data Sovereignty. Journal of Network Security, 21(6), 830-845.

6. Mittal, et al. (2020). Smart KYC Using Blockchain and IPFS. Journal of Information Security and Applications, 5(2), 113-127.

7. Kumari, S. & Gupta, D. (2020). Designing a Framework for Digital KYC Processes Built on Blockchain-based Self-Sovereign Identity. Journal of Blockchain and Cryptocurrencies, 4(1), 98-112.

8. Chen, (2018). KYC Optimization Using Distributed Ledger Technology. Journal of Financial Technology, 2(3), 214-229.

9. Li, et al. (2018). KYC Optimization using Blockchain Smart Contract Technology. Journal of Blockchain Innovations, 3(4), 159-176.

10. Mistry, et al. (2019). Optimizing e-KYC Process Using Distributed Ledger Technology and Smart Contracts. Journal of Technology in Banking, 6(1), 54-69.

11. Abdullah Al Mamun, et al. (2019). Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology. International Journal of Banking and Finance, 15(2), 188-202.

12. Praditya Patil, et al. (2022). Blockchain-based Decentralized KYC Verification Framework for Banks. Journal of Banking Innovations, 9(1), 10-25.