Block Chain Report

Submitted in partial fulfillment of the requirements

Of

POST GRADUATE DIPLOMA

IN

BIG DATA ANALYTICS

KYC REGISTRATION

Ashutosh Pandey	B2020071
Mohammad Anzar Asif	B2020086
Vineeth Nair	B2020090
Souvik Das	B2020118
Tarun Thomas	B2020119
Vaibhav Srivastava	B2020121

GOA INSTITUTE OF MANAGEMENT

SANQUELIM - GOA

Batch: **2020-2022**

Abstract

Know Who You're Dealing With, also known as, KYC allows banks to gain a better understanding of their consumers and their financial transactions. The problem faced is when the consumer has to fill its KYC each time he goes on a platform where the identity of the consumer is essential. Also, the platform where the consumers are to be identified also have to initialize the whole KYC process if the customer is new. Traditional KYC systems rely on a centralized database server, which is vulnerable to cyber-attacks and password leaks and lack of mutual trust. The risk involved here is also to combat the laundering of illicit funds derived from terrorism, organised crime, and drug trafficking. Adoption of blockchain technology is the right solution to these challenges, as shown in a variety of use cases today. The primary goals of blockchain technology have been to increase security and eliminate the need for a third party to monitor system transactions. The purpose of the proposed solution is to create and deploy a peer-to-peer KYC platform based on blockchain technology. KYC is primarily used by governments and businesses to track customers for unlawful and money laundering activities. Furthermore, KYC allows banks to gain a better understanding of their consumers and their financial transactions. This enables them to better manage their risks and make more informed decisions

.

1. Introduction

1.1 Why this High-Level Design Document?

HLD provides a high-level overview of the entire solution, product, system, platform service, or platform. High-Level-Design (HLD) is an architectural approach that defines architectural design in the context of a larger system.

The primary goal of this document is to add the details required to describe the current project in order to represent a good coding model. This document also intends to aid in the

identification of inconsistencies prior to coding and can be used as a reference for module interactions at the next level.

Elements of HLD:

- Overview Design element
- High level information of every process and stage of the project.
- Outline the user's daily process flow and performance needs
- Includes the project's design elements and architecture.

1.2 Scope of HLD

The High-Level Design documentation presents the structure of the system as the application/database architecture, application flow and technology architecture. High-Level Design documentation may use some non-technical terms unlike Low Level design which should be strictly technical jargon.

2. General Description

2.1 Product Perspective

Know your Customer aka KYC originated as a standard to fight against the laundering of illicit money flowing from terrorism, organized crime and drug trafficking. The main process behind KYC is that government and enterprises need to track the customers for illegal and money laundering activities. Moreover, KYC also enables banks to better understand their customers and their financial dealings. This helps them manage their risks and make better decisions.

Using a decentralized KYC system an immutable distributed ledger can be maintained for everyone to access in the network. Every participant interacts with the blockchain using a public-private cryptographic key combination.

By using this system, the time and working hours of a traditional KYC system can be reduced. Since the record is immutable once verified by other banks providing privacy and security

3. Problem Statement

To create a solution using blockchain for KYC verification process of Banks and to implement the following use case:

• To keep the customer personal details confidential

• To authenticate the customers identification for any transactions as requested

• To implement the following blockchain in the following 4 sectors:

1. **Customer Admittance**
2. **Customer Identification**
3. **Monitoring of Bank Activities**
4. **Risk Management**

• To implement distributed data collection

• To deal with fraudulent activities

Real time data upgradation and collection

Faster processing times

4. Proposed Solution

The blockchain is an immutable distributed ledger that is shared by all network participants. A public-private cryptographic key combination is used by each participant to interact with the blockchain. Furthermore, immutable record storage is offered, which is extremely difficult to tamper with.

Banks can take advantage of Blockchain's features to alleviate the challenges associated with the traditional KYC process. A distributed ledger connecting all banks can be set up, where one bank can upload a customer's KYC and other banks can vote on the legitimacy of the customer's details. Customers' KYC will be immutably kept on the blockchain and available to all of the blockchain's banks.

5. Tools used

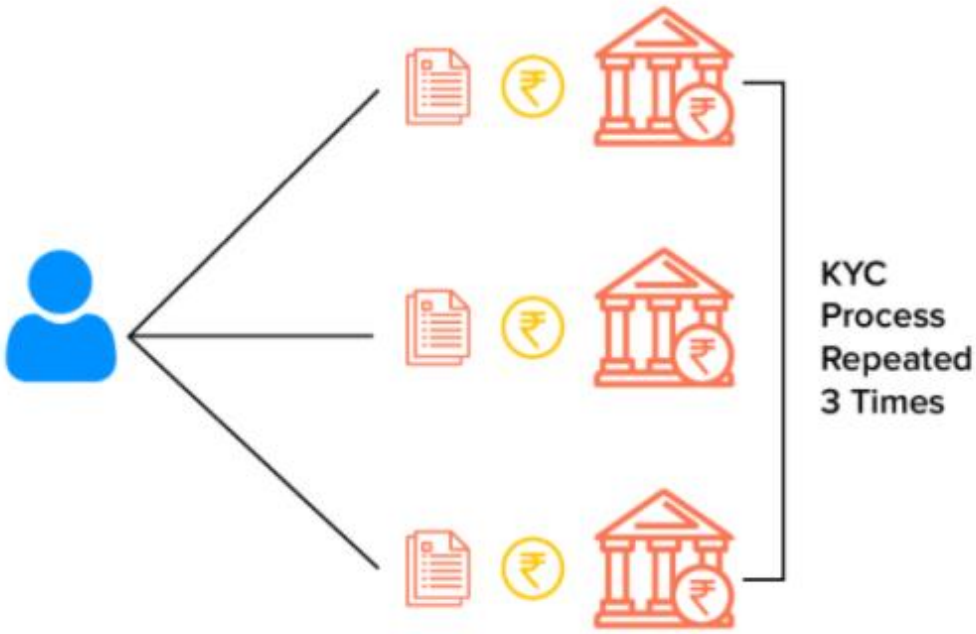
Tools used in this project are:

I. Python
II. Jupyter
III. GitHub

6. Constraints and current challenges

Limitation in the existing KYC functionality:

The KYC practices vary by the institution as there are no global standards. This leads to redundant work and limits the ability for different financial institutions to collaborate to verify identity.



Customers are subject to time-consuming and difficult-to-accomplish onboarding processes when opening new accounts. There are changes in the regulations and this is creating costly and effort-intensive obligations for companies to comply. Also, the customer information is not being updated in material changes, which causes inaccurate information in many bank systems.

Some of the challenges in KYC are:

1. The disparity in Specifications for KYC

   Every bank has their own KYC process setup and customers need to do the KYC again and again for each bank.

   Due to lack of KYC standards, compiling reach request is time-consuming.
2. Adverse impact on Customer relationship.

   It becomes irksome for the customers to provide the same information to different banking entities and industries.

   Banks sometimes even follow up with customers to get more details for KYC.

3. Escalating Costs and Time for Banks

   A recent study concluded that overheads of KYC in a bank increase the onboarding cost for a customer by 18% and the minimum time required to 26 days.

7. Assumptions

In the current solution using blockchain, one of the banks can update the KYC of a customer and the other banks can access the same. This reduces the time consumed in the process also the redundant process which is carried out.

When the user has to update the details after the KYC process, the bank does the verification and is updated in the blockchain properly.

All the banks have access to the system and it cannot be tampered by an individual.

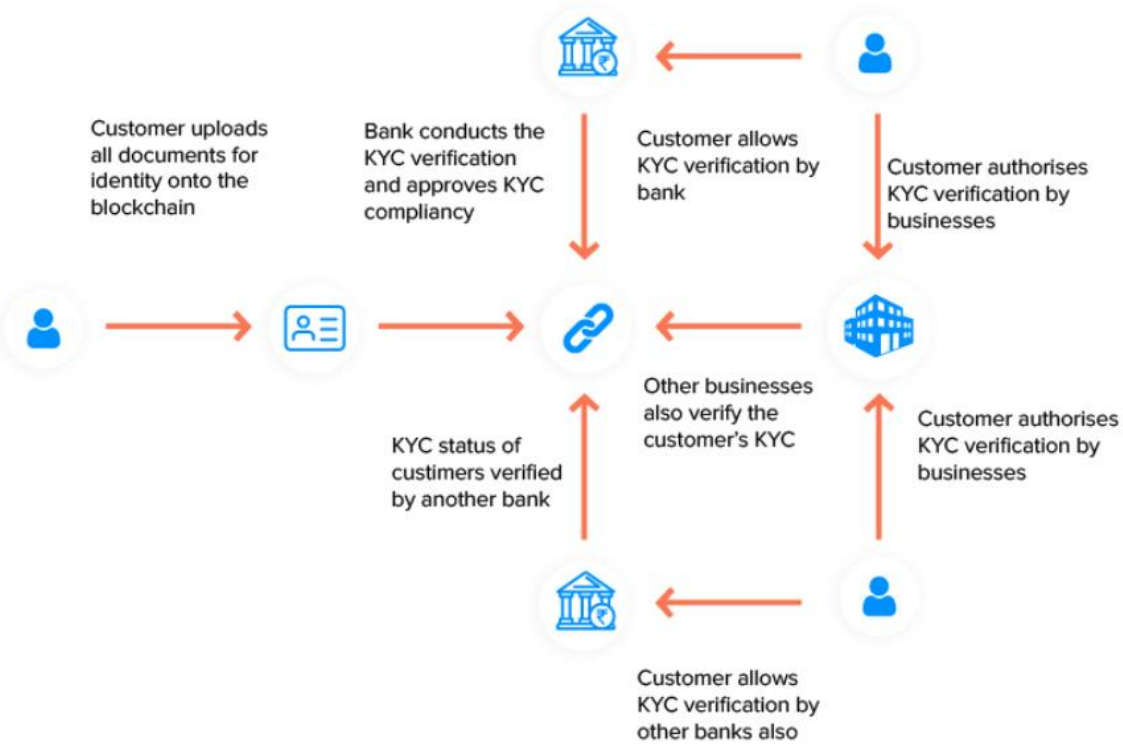
8. KYC Blockchain Implementation

In the traditional KYC system, each bank conducts its own identification check, which means that each user is scrutinized by a separate organization or government body. As a result, confirming each identification from scratch is a waste of time.

We will be able to aggregate information from many service providers into one cryptographically secure and unchangeable database using the blockchain architecture and DLT, which eliminates the requirement for a third party to validate the legitimacy of the knowledge. It enables the creation of a system in which the user only needs to go through the KYC procedure once to authenticate his or her identity.

9. Design Details

1. Process Flow – The Blockchain KYC Process



The process of using Blockchain for KYC happens through multiple stages in a Distributed Ledger Technology.

Let's take a look into the high-level understanding of the steps of how can Blockchain help KYC.

Proposed methodology

Step 1: The user builds a profile on the KYC DLT system

A Blockchain-based KYC platform is deployed by a financial institution (FI), which the user completes as a one-time setup using their identification papers. The data becomes accessible to the FI1 for verification purposes after it has been submitted.

There are multiple options when it comes to storing the users' data:

- A centralized, encrypted server
- On F1s private server
- DLT platform

Step 2: User performs transactions with FI1

When a user completes a transaction with FI1, they grant FI1 access to the user's profile. After that, the FI1 checks the KYC data and saves a copy on their server. They then use the DLT platform to post a 'Hash function.'

Finally, FI1 adds KYC digital copies to the user's profile, along with a Hash Function that matches the DLT platform's Hash Function.

If the KYC data is changed, the Hash Function of the KYC data will no longer match the Hash Function uploaded on the DLT platform, alerting the other financial institutions on the blockchain.

Step 3: User performs a transaction with FI2

When FI2 requests KYC from a user, the user gives FI2 access to their user profile. The KYC data (and its Hash Function) is then compared to the Hash function submitted by FI1. If the two matches, FI2 will know that the KYC obtained by FI1 is the same.

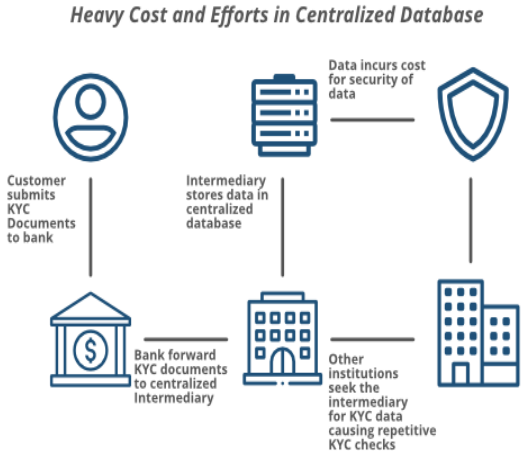
FI2 would have to manually check KYC papers if the Hash Functions did not match.

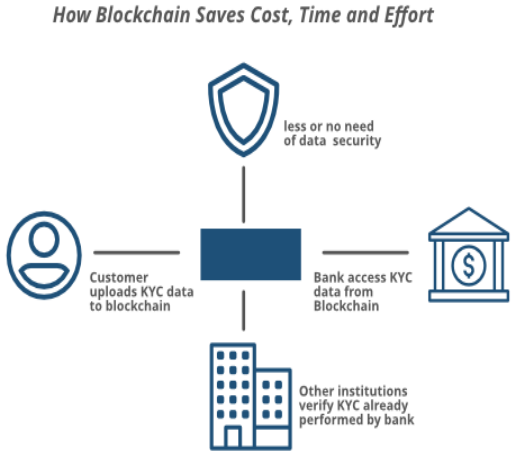
But what if the user gets a new passport or driver's license, and the original document in their DLT user profile changes?

In such circumstances, financial institutions employ smart contracts to update their systems immediately when the user submits new papers. The user sends the updated document to F1, who then broadcasts it over the blockchain (using the new Hash Function), making it available to other FI members.

The benefit of a Blockchain solution for KYC can be seen in:

- **Data Quality:** all data alterations are tracked and monitored in real-time
- **Lowered turnaround time:** through KYC Blockchain software solutions, FIs get direct access to the data which saves data gathering & processing time
- **Reduced manual labor:** KYC on Blockchain eliminates paperwork from the process.





10. LLD for KYC Registration

Know-Your-Customer (KYC) refers to the steps taken by a business to establish customer identity, understand the nature of a customer's activities and to assess risks (if any) involved with the customer. It is a legal requirement for the financial institutions for on-boarding a customer. KYC requires the submission of the identity documents by the customer to the businesses or organizations on which they wish to onboard. Individual verification of the documents is done and thus establishing the identity of the customer independently.

Know your Customer aka KYC originated as a standard to fight against the laundering of illicit money flowing from terrorism, organized crime and drug trafficking. The main process behind KYC is that government and enterprises need to track the customers for illegal and money laundering activities. Moreover, KYC also enables banks to better understand their customers and their financial dealings. This helps them manage their risks and make better decisions.

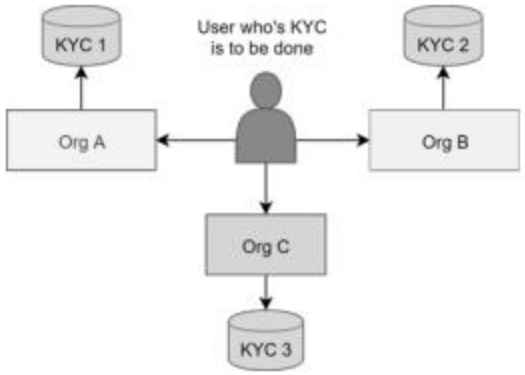


Fig. 1. Current KYC Implementation

Using a decentralized KYC system an immutable distributed ledger can be maintained for everyone to access in the network. Every participant interacts with the blockchain using a public-private cryptographic key combination.

11. Problem Statement

To create a solution using blockchain for KYC verification process of Banks and to implement the following use case:

• To keep the customer personal details confidential

• To authenticate the customers identification for any transactions as requested

• To implement the following blockchain in the following 4 sectors:

5. **Customer Admittance**
6. **Customer Identification**
7. **Monitoring of Bank Activities**
8. **Risk Management**

• To implement distributed data collection

• To deal with fraudulent activities

Real time data upgradation and collection

Faster processing times

12. Proposed Solution

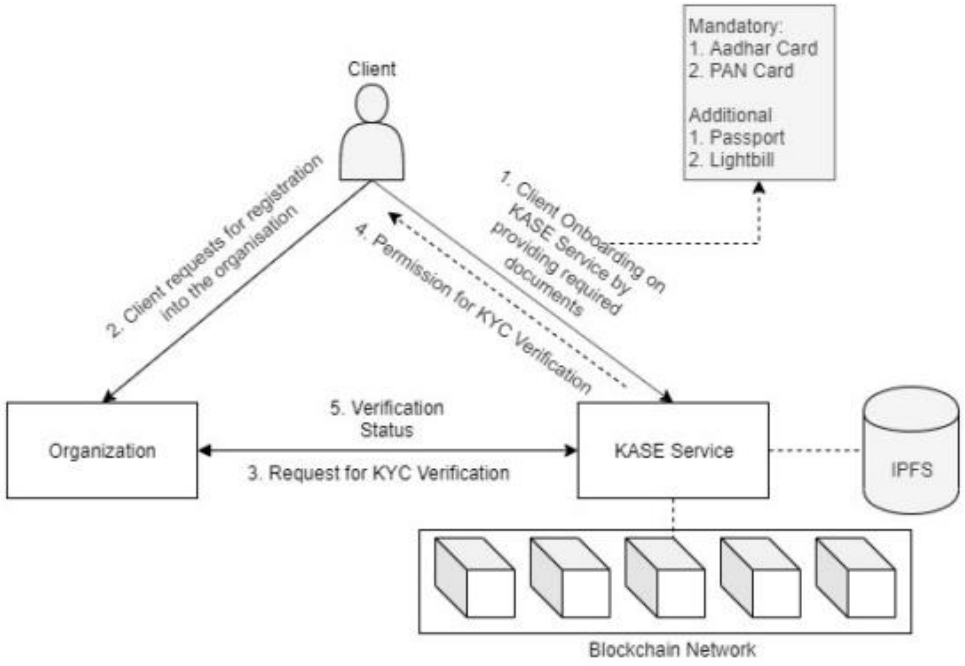
The blockchain is an immutable distributed ledger that is shared by all network participants. A public-private cryptographic key combination is used by each participant to interact with the blockchain. Furthermore, immutable record storage is offered, which is extremely difficult to tamper with.

Banks can take advantage of Blockchain's features to alleviate the challenges associated with the traditional KYC process. A distributed ledger connecting all banks can be set up, where one bank can upload a customer's KYC and other banks can vote on the legitimacy of the customer's details. Customers' KYC will be immutably kept on the blockchain and available to all of the blockchain's banks.

This mechanism allows the blockchain to enforce “smart contracts” such that the transactions are only committed to the blockchain after certain conditions are satisfied.

The system initially asks the user to register on the service and provide his information, including identity proofs to the service voluntarily. The next time the customer wants to get on boarded onto a business he/she uses the service for the KYC process. This information is stored encrypted by the user’s secret key on the distributed file system and the transaction is stored on the blockchain to ensure transparency. If a customer wants to onboard to a business, he/she can register to the business using the service and provide basic details which would be given to the business and verified by the service. The service first asks the customer for confirming and validating the KYC request in accordance with GDPR and then after receiving the permission verifies the customer’s identity to the business. The request transaction is also pushed onto the blockchain to ensure transparency of the data flow and credibility of the transfer. The service also provides businesses the feature of verification of any KYC documents they may request based on their internal

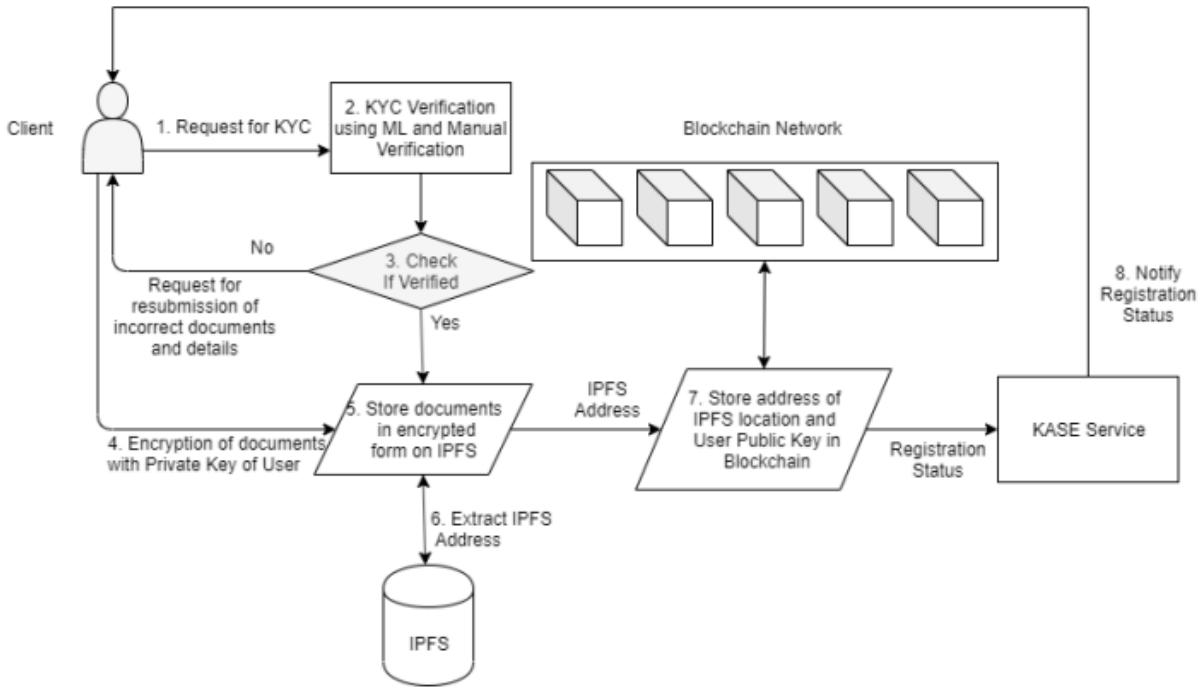
policies and uses Machine Learning approaches to verify those documents and to confirm the identity of the individual



13. Architecture Description

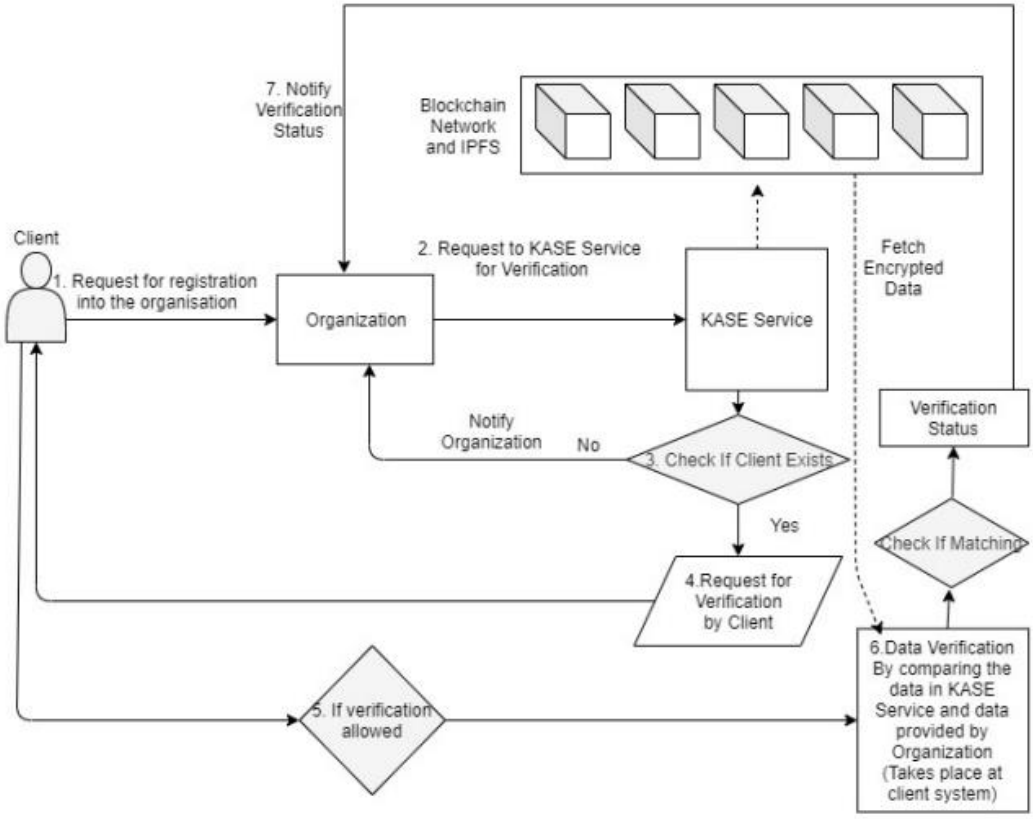
At the time of on-boarding onto the system (KASE), the user will have to provide his identity proofs he/she has. The user will have to fill in all the details manually also, which will be converted to a JSON object. The data entered by the user and data extracted from the documents uploaded will cross checked for any irregularities using machine learning, and an extra layer of verification can be added by comparing the images of the user on various IDs and their image taken digitally. Once all the checks are complete and all the data is verified, a public-private key pair is generated on the user's system. For security purposes the private key will be a key-file which could be stored on an isolated storage device such as a USB drive or a Gemalto Token. The data stored in JSON object will be stringified so that it can be stored in IPFS along with the various ID documents, which are encrypted using the user's public key and stored on IPFS. All the documents that will be uploaded will have a different hash. The JSON file will also have a different hash.

All these set of hashes will along with the username will be stored in Ethereum blockchain as a “KYC on-boarding request”. The Ethereum wallet address generated will be of 42 characters which is impossible to remember. A mapping functionality provided by Solidity can be used to map username with the wallet address. At the time 5 of data retrieval, the user has to only provide his unique username to access his/her details. From username, the wallet address can be accessed and through that one can get their stored data



User Onboarding Process

If a business wants to do the KYC of a customer, it can use the proposed service in two ways: 1. It can either request directly for verification 2. It can request the customer for documents and get those verified with the service. When the business wants to KYC a customer, the business sends a request to the customer to allow the KYC to be processed by the business. KASE sends a notification to the user that the business is requesting KYC and the customer has to authenticate and allow the service to use the user’s information to verify it to business. The system gets the address of the user’s encrypted information from the blockchain and uses it to verify the customer details provided. After completing the request, the system pushes a “request transaction” to the blockchain.



KYC Process

Technical Flow:

13.1 Importing Libraries:

Importing of required libraries need to be done in order to create Blockchain and do necessary mining.

13.2 Block Creation:

Block is a data structure used for keeping a set of transactions which is distributed to all nodes in the network. We need to create a block and set it up by initialising some of the functions. In order to create block, we need to create Genesis Block, Nonce Block and Hash Key.

13.3 Transaction creation:

It is a smallest building block of a blockchain system (records, information, etc.) that serves as the purpose of blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger.

13.4 Consensus Protocol:

It is proof of work where we need to set rules and arrangements to carry out blockchain operations. If everyone abides by them, they become self-enforced inside the blockchain.

13.5 Mining:

It is a block verification process before adding anything to the blockchain structure. Nodes interact via private/public keys. They use private key to sign their transactions and public key to address on network. The neighboring peers make sure this incoming transaction is valid before relaying it any further in network.

13.6 Blockchain Creation:

It is a process of creating a sequence of blocks in a specific order. Once a new block is created, it is sent to each node within the blockchain system. Then, each node verifies the block and checks whether the information stated there is correct. If everything is alright, the block is added to the local blockchain in each node.

14. Conclusion and Future Scope

Blockchain is one of the latest technologies in the field of cybersecurity and ensures trust in trustless environments. The proposed Blockchain-Based KYC system that uses a decentralized database , for Legacy KYC processes. Through blockchain, KASE ensures that the parties using the service can trust the service and its reliability, and will use it over other solutions. The solution further uses a decentralized file store to ensure complete decentralization of data and reduce any single points of failure. Our prototype implementation through Solidity smart contracts gives encouraging results. KASE Service can be used as a one stop solution of all KYC needs. By leveraging the power of ML, AI and explainable AI we can make the system free of manual verification

15. References

- https://www.nasdaq.com/articles/how-blockchain-can-help-upgrade-kyc-processes-2021-05-05
- https://www.geeksforgeeks.org/blockchain-and-kyc/
- https://appinventiv.com/blog/use-blockchain-technology-for-kyc/