11. 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.

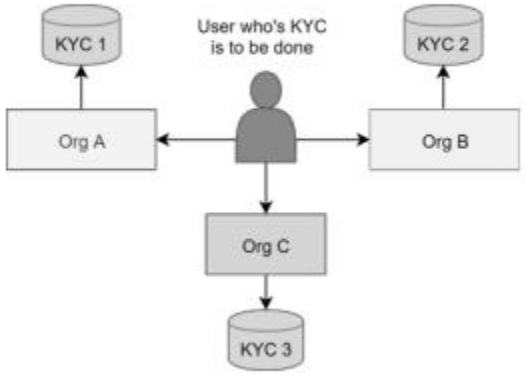


Fig. 1. Current KYC Implementation

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.

12. 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

13. Proposed Solution

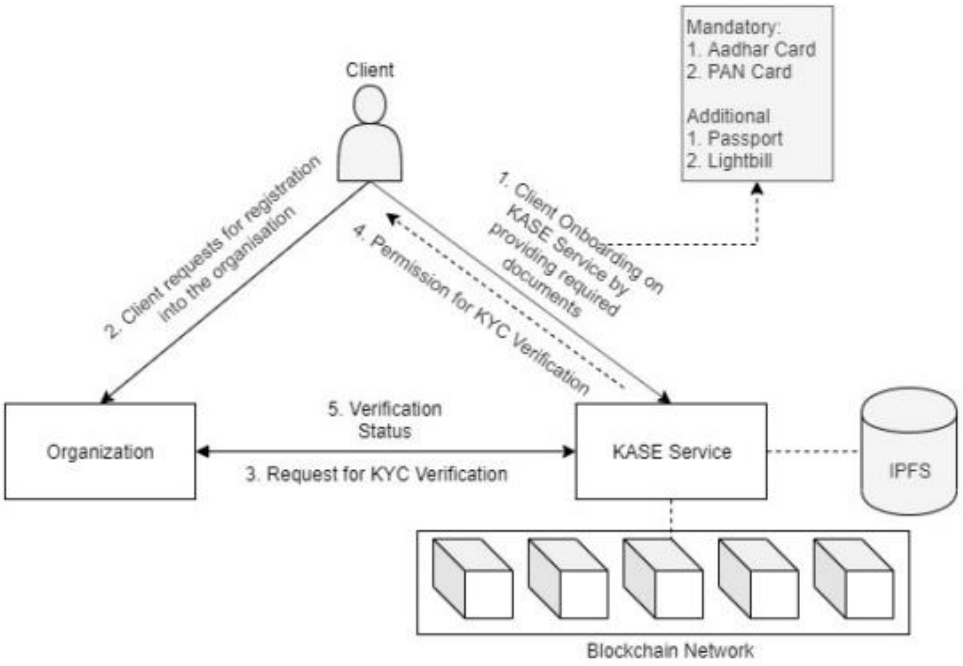
The blockchain is an immutable distributed ledger that is shared by all network participants. A public-private cryptographic key combination is used by each participant to interact with the blockchain. Furthermore, immutable record storage is offered, which is extremely difficult to tamper with.

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.

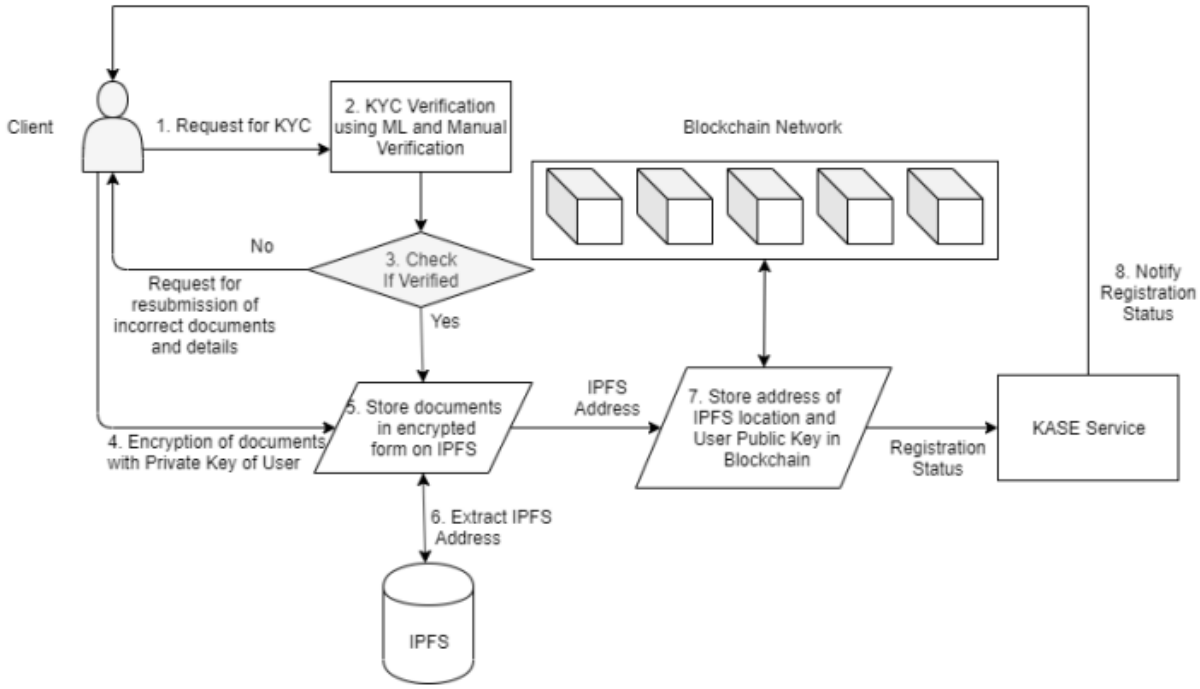
The system initially asks the user to register on the service and provide his information, including identity proofs to the service voluntarily. The next time the customer wants to get on boarded onto a business he/she uses the service for the KYC process. This information is stored encrypted by the 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



14. Architecture Description

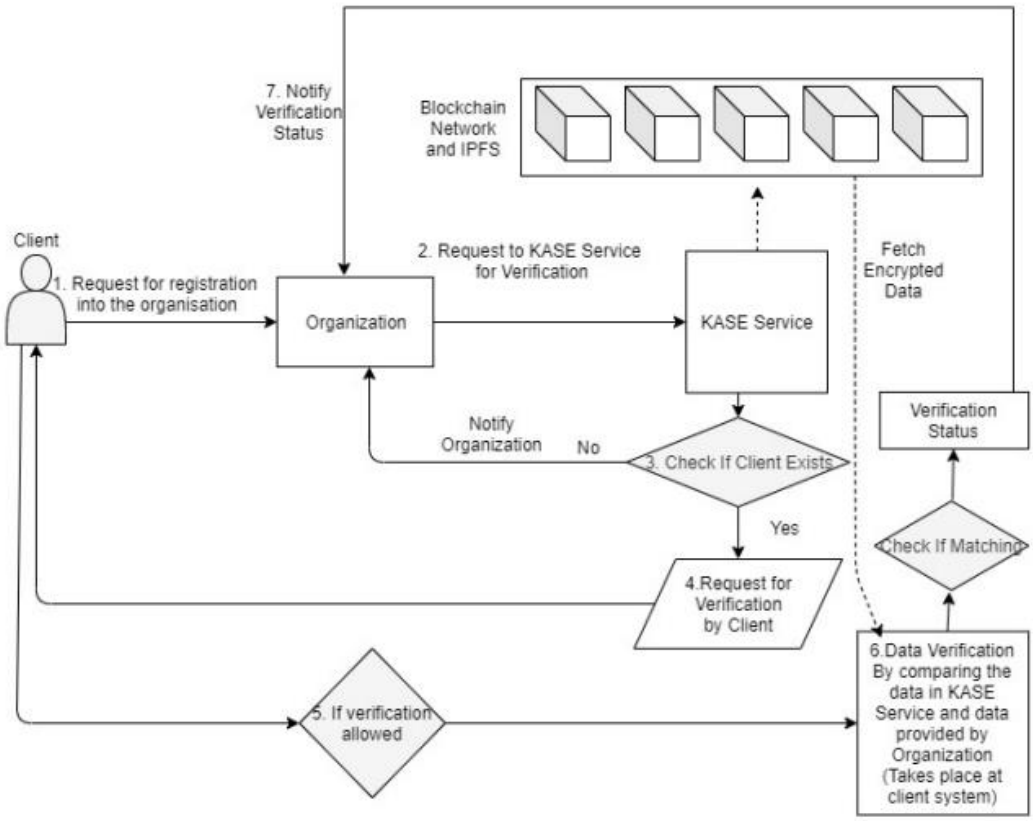
At the time of on-boarding onto the system (KASE), the user will have to provide his identity proofs he/she has. The user will have to fill in all the details manually also, which will be converted to a JSON object. The data entered by the user and data extracted from the documents uploaded will cross 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:

14.1 Importing Libraries:

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

14.2 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.

14.3 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.

14.4 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.

14.5 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 neighbouring peers make sure this incoming transaction is valid before relaying it any further in network.

14.6 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.

15. 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

16. 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/