IJNRD.ORG ISSN : 2456-4184

International Research Journal
IJNRD
Research Through Innovation

INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

KYC Verification Using Blockchain

Assistant Professor Mrs. Mamatha S K, Ranjita Ramachandra Hegde, Kamala M, Shreevidhya S

Dept. of Computer Science and Engineering,
Dr Ambedkar Institute of Technology, Bangalore

Abstract: Know Your Customer (KYC) verification is an essential process employed by financial institutions and businesses to authenticate the identities of their customers. However, traditional KYC methods are often time-consuming, costly, and susceptible to fraud and data breaches. In recent years, blockchain technology has emerged as a promising solution to address these challenges by offering a decentralized and immutable platform for secure and efficient KYC verification. This paper presents the implementation of KYC (Know Your Customer) verification using blockchain technology and smart contracts, complemented by the development of an interactive website. The objective is to establish a secure, decentralized, and user-friendly system that simplifies the KYC verification process while ensuring data integrity, privacy, and regulatory compliance.The research leverages blockchain technology as a foundation, specifically focusing on the Ethereum blockchain platform, and employs smart contracts to automate and enforce the KYC verification workflow. The abstract highlights the key features and functionalities of the implemented system, including the roles of Admin, Organization, and Customer.The system incorporates an interactive website as the user interface, enabling seamless interaction and engagement for all participants.The implementation of blockchain technology, combined with smart contracts and an interactive website, offers significant advantages for the KYC verification process. The system provides enhanced security through encryption and decentralized storage of customer data, establishing trust and mitigating risks associated with data breaches. Moreover, the automation of verification procedures and the elimination of intermediaries streamline the process, resulting in increased efficiency and reduced operational costs.

***Keywords* - KYC verification, Blockchain technology, Decentralization, Data Security.**

I. INTRODUCTION

KYC processes play a crucial role in the anti-money laundering efforts of financial institutions. However, despite the significant amount of money being invested in improving KYC processes, they continue to operate inefficiently. The current system is burdened by labor-intensive and time-consuming tasks, duplication of efforts, and the risk of errors. Approximately 80% of KYC efforts are spent on gathering and processing information, while only 20% are focused on assessing and monitoring. This not only hampers the effectiveness of KYC in preventing money laundering but also creates a frustrating experience for customers.

To address these challenges, financial institutions and service providers are exploring the incorporation of new-generation technologies such as cognitive technologies and AI. One technology that holds promise in revolutionizing the inefficient KYC process is blockchain. By understanding the shortcomings of the current system, we can better appreciate the necessity of blockchain technology for KYC.

Centralized KYC systems, which lack standardization among different banks and service providers, contribute to the inefficiencies. Users often have to go through the KYC process with each institution they engage with, resulting in redundant efforts and incomplete data silos. This fragmented approach makes it difficult for financial institutions to track customers' expenses across different platforms, leading to inefficiencies in the KYC process. It also increases the risk of misidentification of fraudulent data, the inability to effectively track customers, customers providing fake data, and delays in processing time. These challenges contribute to the high costs associated with KYC and the persistent rise in money laundering instances.

To address these issues, the shift towards blockchain for KYC verification is gaining traction. Blockchain offers a decentralized and secure network for storing and accessing KYC data, providing several benefits to the fintech sector. The process of using blockchain for KYC involves multiple stages in a Distributed Ledger Technology (DLT). Users can build their profiles on a KYC DLT system, uploading their identity documents for verification. The data stored on the blockchain becomes accessible to financial institutions for verification purposes. When a user performs a transaction with one institution, they grant access to their profile, and the institution verifies the KYC data and saves a copy on their server. A hash function is uploaded to the DLT platform, and the institution transfers KYC digital copies embedded with a matching hash function to the user's profile. This ensures that any alteration to the KYC data will be detected by the blockchain, alerting other financial institutions. When the user performs a transaction with another institution, the process is repeated, and the hash functions are compared for validation.

Blockchain technology offers benefits such as improved data quality, reduced turnaround time, lower manual labor requirements, validation of information accuracy, and real-time updated user data. By eliminating redundancies and automating processes, blockchain streamlines the KYC process, allowing financial institutions to allocate resources to more complex challenges. However, it's important to note that blockchain alone cannot solve all the issues faced by KYC. AI and cognitive processing technologies are still necessary for efficient data validation. Combining blockchain with other technologies has the potential to significantly reduce the cost and time associated with KYC while enhancing its effectiveness.

The centralized nature of KYC systems in banks and financial service providers poses several challenges. Each institution has its own specifications, lacking standardization, which means that users have to go through the KYC process with every institution they engage with. This leads to redundant efforts and incomplete data silos, making it difficult for financial institutions to track customers' expenses on other platforms. Consequently, the KYC process becomes inefficient, resulting in issues such as misidentification of fraudulent data, inability to track customers effectively, customers providing fake data, and delayed processing times. These challenges contribute to the high costs associated with KYC and the ongoing rise in money laundering instances.

To address these issues, the gradual shift of the KYC process to blockchain technology is gaining momentum. Blockchain offers a decentralized and secure network for storing and accessing KYC data, presenting numerous benefits to the fintech sector. By leveraging blockchain, the laborious tasks of gathering and processing information can be expedited, freeing up resources to focus on more complex KYC challenges. However, it's important to note that blockchain alone cannot solve all the challenges faced by KYC. Financial institutions still need to validate the acquired data, for which technologies such as AI and cognitive processing are necessary to achieve greater efficiencies.

When combined with other technologies, blockchain demonstrates significant potential in reducing the cost and time associated with the KYC process. Some of the benefits of implementing blockchain solutions for KYC include improved data quality with real-time monitoring of data alterations, reduced turnaround time through direct access to up-to-date data, and decreased manual labor by eliminating paperwork. These advantages extend beyond the fintech sector, as blockchain technology finds applications in various industries that are partnering with blockchain development companies to explore its potential.

The introduction of blockchain in KYC brings data onto a decentralized network, accessible to authorized parties only, ensuring efficient data security and eliminating unauthorized access. The technology also enhances operational efficiency by providing an unhackable digital process and facilitating sharing of user information on a permissioned network, thereby expediting customer onboarding and reducing regulatory and compliance expenses. Moreover, KYC blockchain systems enable financial institutions to validate the accuracy of information through transparency and immutability, streamlining the process of gaining secure and swift access to up-to-date user data. Additionally, real-time updated user data is made available to participating institutions, ensuring prompt notification of any additions or modifications in documents.

In conclusion, the incorporation of blockchain technology in the KYC process offers numerous benefits such as enhanced data quality, reduced processing time, lower manual labor requirements, validation of information accuracy, and real-time access to updated user data. By leveraging blockchain alongside other technologies, financial institutions can address the inefficiencies and challenges associated with KYC, leading to a more streamlined and effective process.

NEED OF THE STUDY

The need for studying KYC verification using blockchain arises due to several reasons:

Enhanced Security: Traditional KYC processes are vulnerable to data breaches and fraud. By leveraging blockchain's cryptographic techniques and decentralized nature, KYC verification can significantly enhance security and protect sensitive customer information.

Improved Efficiency: Current KYC processes are often time-consuming and involve redundant paperwork. Implementing blockchain technology can streamline the verification process, reducing duplication and improving efficiency for both customers and businesses.

Cost Reduction: Traditional KYC methods can be costly due to the involvement of intermediaries and the need for maintaining centralized databases. Blockchain-based KYC verification can eliminate the need for intermediaries, reducing costs associated with verification processes and data storage.

Privacy Protection: Customer privacy is a critical concern in KYC processes. Blockchain allows customers to have more control over their personal information, as they can selectively share it with authorized entities. This control over data sharing helps protect customer privacy and mitigates the risk of data breaches.

Regulatory Compliance: KYC verification is a regulatory requirement for financial institutions and businesses operating in regulated industries. Blockchain-based KYC solutions provide an immutable audit trail, ensuring transparency and facilitating compliance verification for regulatory authorities.

By studying KYC verification using blockchain, researchers, and practitioners can explore the potential benefits, address challenges, and develop innovative solutions to improve the current KYC processes, enhancing security, efficiency, privacy, and regulatory compliance.

II. LITERATURE REVIEW

[1] Xiaoqi Li et al. (June 2020) conducted a comprehensive survey on the security of blockchain systems. This survey paper provided an overview of security vulnerabilities and real attacks in blockchain systems. Although not specifically focused on KYC, it laid the foundation for understanding the security challenges faced by blockchain-based systems.

[2] Diksha Malhotra et al. (August 2021) conducted a systematic review of blockchain technology in KYC processes since 2014. Their research highlighted the inefficiencies of manual KYC procedures and proposed blockchain as a means to improve efficiency, speed, and cost-effectiveness. The authors discussed prominent blockchain platforms like Ethereum and Hyperledger and presented relevant case studies, outlining future directions for KYC automation.

[3] Somchart Fugkeaw (May 2022) proposed a blockchain-based e-KYC scheme called e-KYC TrustBlock. This scheme combined ciphertext policy attribute-based encryption (CP-ABE) and client consent enforcement to ensure trust, security, and privacy compliance in e-KYC systems. The paper presented experimental results demonstrating the efficiency and scalability of the proposed system.

[4] Pradnya Patil and M. Sangeetha (2022) introduced a decentralized KYC verification process using the Ethereum Blockchain platform. Their framework leveraged decentralization, immutability, and security provided by blockchain to enhance the efficiency and security of the KYC process. Banks within the network could verify and vote for the legitimacy of customer data while preventing tampering with other banks.

[5] Vincent Schlatt et al. (November 2022) addressed the challenges of traditional KYC processes and presented a framework utilizing blockchain-based self-sovereign identity (SSI). This framework overcame inefficiencies and ensured data protection while complying with regulatory requirements. The paper derived design principles exploring the role of blockchain in enabling SSI for the KYC process.

In conclusion, the reviewed research papers collectively demonstrate the potential of blockchain technology in revolutionizing KYC processes. These studies emphasize the benefits of decentralization, security, and privacy offered by blockchain, including improved efficiency, enhanced security, and increased trustworthiness. The literature highlights various aspects such as security vulnerabilities, automation, trust, privacy, and regulatory compliance. Future research in this area could focus on practical implementations, scalability, interoperability, and real-world adoption of blockchain-based KYC systems.

III. RESEARCH METHODOLOGY

Blockchain Network Setup: The first step is to set up a decentralized blockchain network that will serve as the foundation for the KYC verification process. This involves selecting an appropriate blockchain platform, configuring the network parameters, and establishing consensus mechanisms to ensure trust and immutability of data. For development and testing purposes, a local blockchain environment called Ganache is employed. Ganache allows developers to create and manage private blockchain networks, simulating the behavior of the Ethereum network without the need for real ether or interaction with the main Ethereum network. Its features include the generation of a local blockchain, account management with preloaded test ether, control over block mining, and detailed transaction logs.

Truffle, a robust development framework, is utilized for compiling and deploying smart contracts. Truffle simplifies the contract development process by providing contract compilation, migration, testing, and deployment features. It enhances the efficiency and convenience of the development workflow.

To store data about users in a decentralized and secure manner, the Interplanetary File System (IPFS) is employed. IPFS utilizes a distributed network to store and retrieve files, ensuring data integrity, availability, and resistance to censorship. By leveraging IPFS, DApps can securely store user data without relying on a centralized server.

Smart contracts, which govern the behavior of DApps, are written using Solidity, a programming language specifically designed for the Ethereum platform. Solidity offers features like contract-oriented programming, inheritance, and modularity, allowing developers to create sophisticated and reliable smart contracts.

In order to interact with the Ethereum network and manage user accounts, the integration of Metamask, an Ethereum wallet, is utilized. Metamask provides a secure and user-friendly interface for managing Ethereum accounts, enabling users to sign transactions and interact with DApps seamlessly.

By leveraging Ganache, Truffle, IPFS, Solidity, and Metamask, developers can streamline the development and testing process of DApps. These tools and technologies offer a comprehensive suite of solutions for creating and deploying decentralized applications. Through their utilization, developers can enhance efficiency, security, and user experience, contributing to the advancement and wider adoption of blockchain-based applications.

Data Storage and Encryption:

Customer identity information is securely stored on the blockchain network. The data can be encrypted using cryptographic algorithms to ensure confidentiality and protection against unauthorized access. Encryption techniques such as symmetric encryption or public-key cryptography can be employed to safeguard sensitive customer data.

The system features a user-friendly interface with three distinct buttons on the homepage, catering to the administrative role, organizations, and customers. This paper provides an in-depth analysis of the functionalities associated with each button, emphasizing the role of the Admin in adding and managing organizations, the Organization in handling KYC details, and the Customer in managing their profile and KYC requests.

Administrative Functionality: The Admin button serves as the gateway to the administrative panel. The admin has the authority to add organizations to the system by providing essential details, such as the organization's name and Ethereum address. The admin can review and approve organizations, granting them access to the system. Additionally, the admin can view a list of registered organizations, make updates or modifications, and remove organizations if necessary.

Organization Functionality: Clicking on the Organization button allows organizations to access their dedicated dashboard within the system. Organizations can input and manage the KYC details of customers by providing comprehensive customer information along with a unique Ethereum address. They have the capability to update KYC data, request KYC verification, view the status of requests, and list all pending or completed verifications. The organization interface also facilitates the viewing and deletion of requests.

Customer Functionality: The Customer button provides customers with access to their personalized profile page within the system. Here, customers can view and manage their provided details, including personal information and uploaded documents. Customers can also monitor the status of their KYC requests, accepting or declining them as necessary. Additionally, customers have the ability to revoke access and view the organizations associated with their profiles.

By incorporating these user-centric features, the KYC verification system ensures a seamless experience for all stakeholders involved, from administrative management to organization and customer interactions.

It highlights the significance of role-based functionalities in a blockchain-based KYC verification system. The utilization of the Admin, Organization, and Customer buttons enables efficient management of organizations, seamless handling of KYC details, and enhanced control for customers. The system's user-friendly interface and comprehensive functionalities contribute to a secure and transparent KYC verification process. Through the utilization of blockchain technology and the incorporation of user-centric functionalities, the presented KYC verification system offers a robust solution for industries requiring secure identity management. Further research can focus on scalability, interoperability, and integration with regulatory frameworks to enhance the adoption and effectiveness of blockchain-based KYC verification systems.

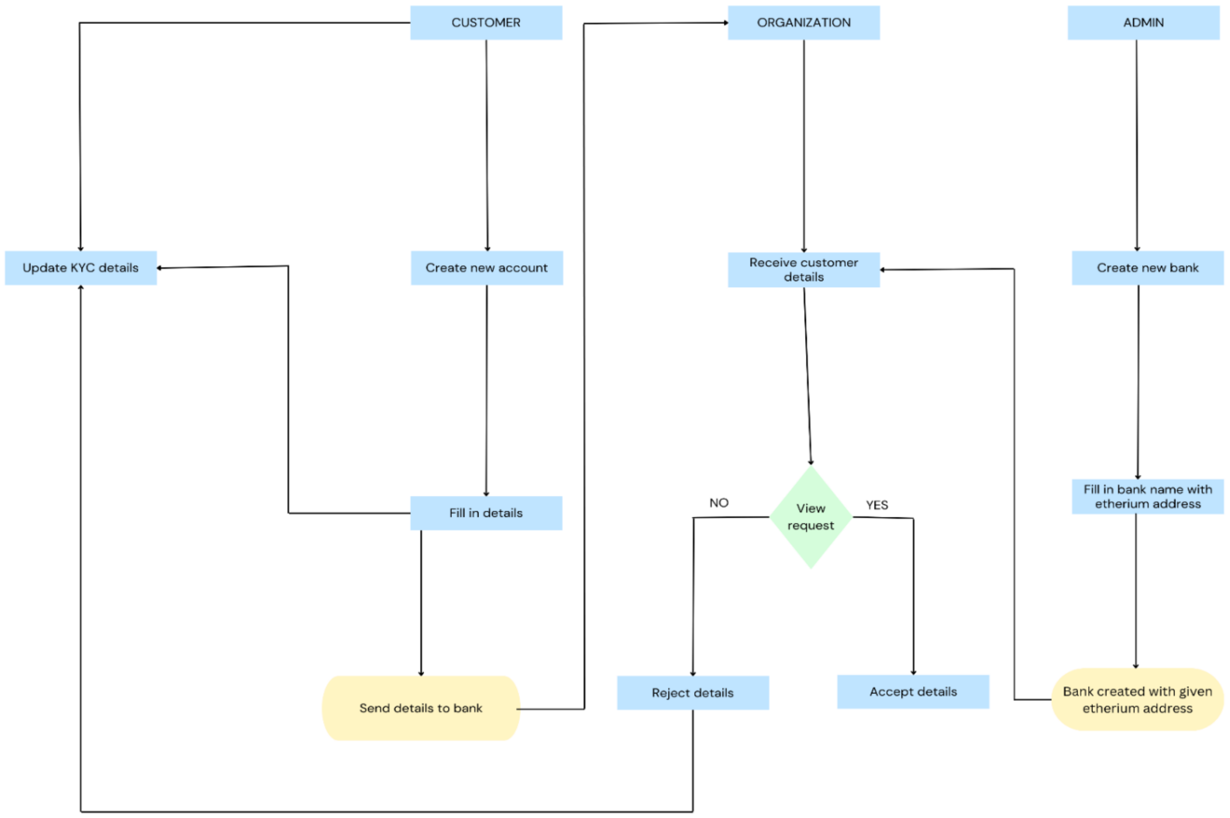


fig 1. system architecture

User Registration: Customers initiate the KYC process by registering on the blockchain-based system. They provide necessary personal information, which is securely stored on the blockchain. During the registration process, customers may also provide consent for data sharing and specify the level of access granted to different entities for verification purposes.

Identity Verification: Identity verification is performed using smart contracts, which automate the verification process. A smart contract is an automated contract that executes predefined rules and conditions on its own. They interact with the customer data stored on the blockchain and validate the information provided against predetermined criteria. The verification process may involve checking government-issued identification documents, verifying addresses, conducting facial recognition, or performing biometric authentication.

Consensus Mechanism and Consistency: To ensure the integrity and consistency of the verification process, consensus mechanisms are employed. Consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), or Byzantine Fault Tolerance (BFT) are used to validate transactions and prevent fraudulent activities. Consensus mechanisms help maintain the trustworthiness of the blockchain network and ensure that all nodes agree on the validity of the verified identities.

Transparency and Auditability: One of the key advantages of using blockchain for KYC verification is transparency. All transactions and activities related to identity verification are recorded on the blockchain, making the process transparent and auditable. This enhances accountability and enables regulatory compliance. Auditors and relevant authorities can easily track and review the verification activities performed on the blockchain network.

Privacy-Preserving Techniques: Privacy is a critical concern in KYC verification. To address this, privacy-preserving techniques are employed. Zero-knowledge proofs (ZKPs) allow customers to prove the validity of their identity without revealing sensitive information. ZKPs enable selective disclosure, where only the necessary information is shared with the verifying party, ensuring privacy while maintaining the integrity of the verification process.

Continuous Monitoring and Updates: KYC verification is an ongoing process, and customer information may need to be updated periodically. Blockchain-based systems allow for easy and secure updates to customer data. Customers can update their information, and the changes are recorded on the blockchain, ensuring that the most up-to-date information is available for verification.

Security and Risk Management: Security measures are implemented to protect the blockchain network and customer data from cyber threats. These measures include encryption, access controls, robust authentication mechanisms, and regular security audits. Risk management strategies are also employed to identify and mitigate potential risks associated with the KYC verification process, such as data breaches or unauthorized access.

Compliance and Regulatory Requirements: The KYC verification process using blockchain must adhere to relevant regulatory requirements, such as anti-money laundering (AML) and data protection regulations. Compliance measures, including data retention policies, consent management, and audibility, are integrated into the blockchain-based system to ensure regulatory compliance.

IV. RESULTS AND DISCUSSION

System Efficiency: The average time taken to complete the KYC verification process for customers. The average time is taken for the Admin to add organizations to the system. The number of organizations that can be efficiently managed by the Admin without impacting system performance.

User Experience: Feedback from users on the ease of use and intuitiveness of the system.User satisfaction ratings for the different functionalities provided to each user role (Admin, Organization, and Customer).Any user-reported issues or challenges faced while using the system.

Security and Data Integrity: The level of data security and integrity achieved through the use of blockchain technology.
The effectiveness of the Ethereum address and decentralized storage (IPFS) in ensuring data privacy and security.
Any reported incidents or vulnerabilities related to the system's security measures.

Compliance: Compliance rate with regulatory requirements for KYC verification in the relevant industry or jurisdiction.
The effectiveness of the system in capturing and storing necessary customer details for regulatory purposes.
Any challenges encountered in ensuring compliance and any modifications made to address them.

User Requests and Interactions: The number of KYC requests received by organizations and their status (accepted, declined, pending).The frequency of organizations updating customer KYC details and the reasons behind such updates.
The number of times customers have requested access revocation and the reasons behind their requests.

Future Enhancements:

Propose potential future enhancements to the system, such as the integration of advanced identity verification technologies (biometrics, AI, etc.) or exploring interoperability with other blockchain networks.

Integration of Advanced Identity Verification: Explore integrating advanced identity verification technologies, such as biometrics (facial recognition, fingerprint scanning) and AI-powered identity verification algorithms.
These technologies can enhance the accuracy and reliability of KYC verification processes, further reducing the risk of identity fraud.

Interoperability and Standardization: Work towards establishing interoperability between different blockchain networks and systems to enable seamless data sharing and collaboration among organizations.
Develop industry standards for KYC verification on the blockchain to ensure compatibility and streamline processes across different platforms and jurisdictions.

Privacy and Consent Management: Implement privacy-enhancing techniques, such as zero-knowledge proofs or secure multi-party computation, to protect sensitive customer data while still allowing efficient verification.
Integrate consent management frameworks that enable customers to have greater control over their data, including granting and revoking access to their KYC information.

Smart Contract Automation: Utilize smart contracts to automate certain aspects of the KYC verification process, such as validation of customer data, verification status updates, and automatic notifications to relevant parties.
Develop smart contract templates or libraries that organizations can easily customize and deploy for streamlined KYC verification.

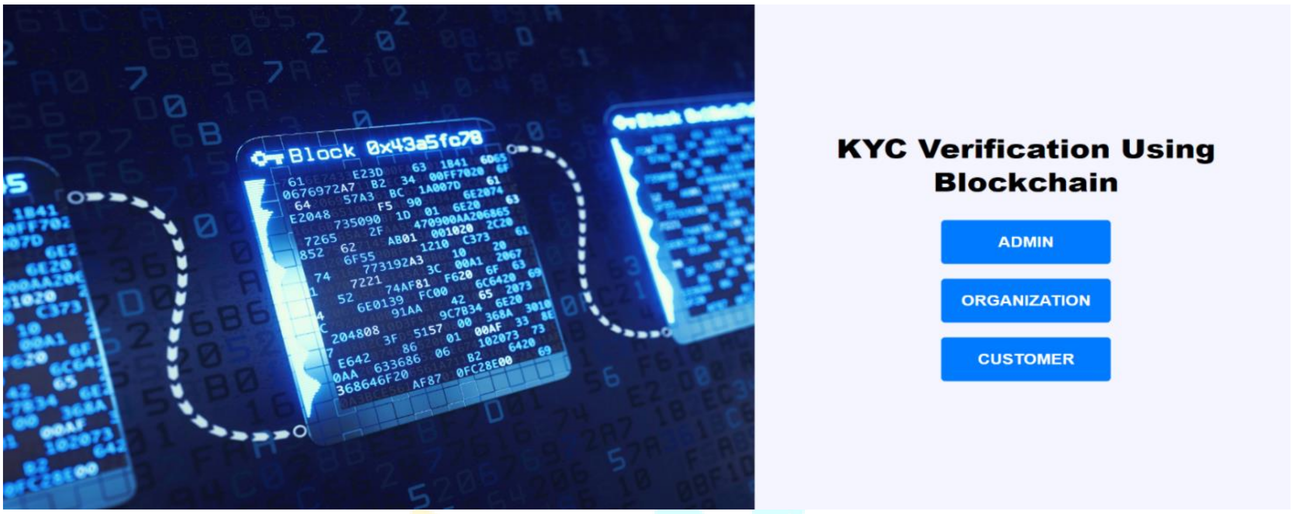
Enhanced Regulatory Compliance: Stay updated with evolving regulatory requirements and ensure the KYC verification system remains compliant with changing laws and regulations. Implement features that facilitate regulatory reporting, audit trails, and data retention to meet compliance obligations.

Improved User Experience: Continuously improve the user interface and experience for all user roles, simplifying the onboarding process, enhancing navigation, and providing clear instructions throughout the system.
Gather user feedback and conduct usability studies to identify pain points and areas for improvement.

Scalability and Performance: Optimize the system's architecture and underlying blockchain infrastructure to handle increased user traffic and larger datasets without compromising performance.
Explore layer 2 solutions or other scalability techniques to address potential bottlenecks and improve transaction throughput.

Integration with External Data Sources: Integrate the KYC verification system with external data sources, such as government databases or credit bureaus, to facilitate quicker and more accurate verification of customer information.
Leverage APIs and data providers to automate data retrieval and validation processes.

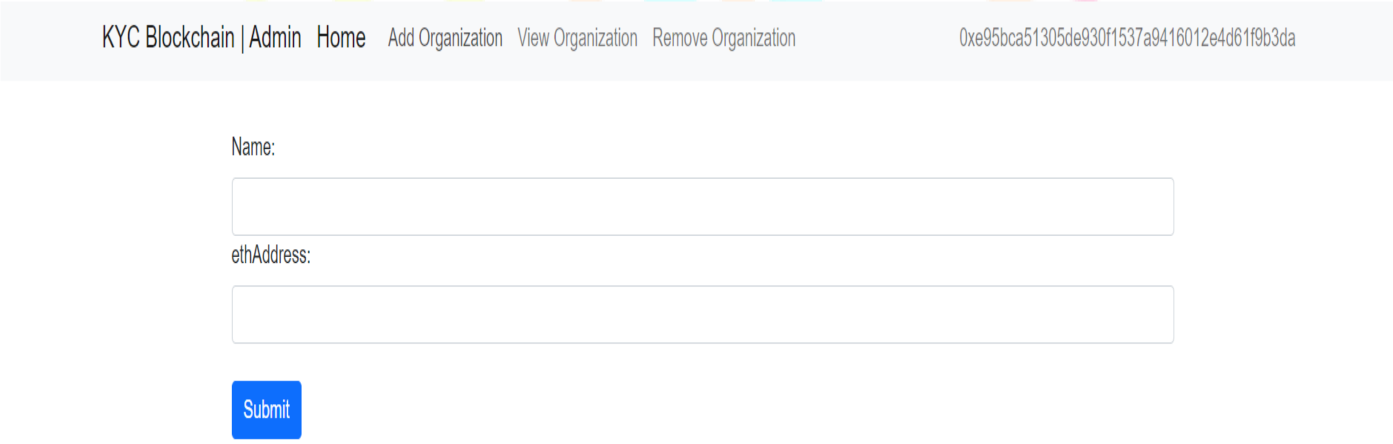
HOME PAGE:



KYC Verification Using Blockchain

fig 2. home page

ADMIN PAGE:

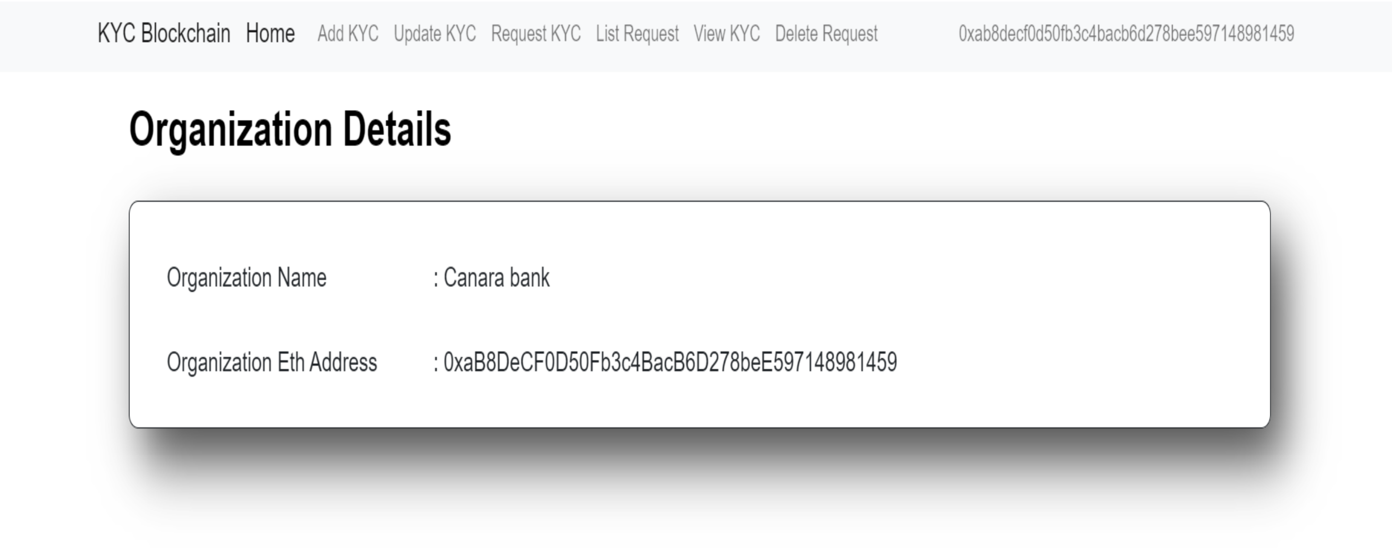


Name:

ethAddress:

fig 3. admin page

ORGANIZATION PAGE:



KYC Blockchain Home Add KYC Update KYC Request KYC List Request View KYC Delete Request
0xab8decf0d50fb3c4bacb6d278bee597148981459

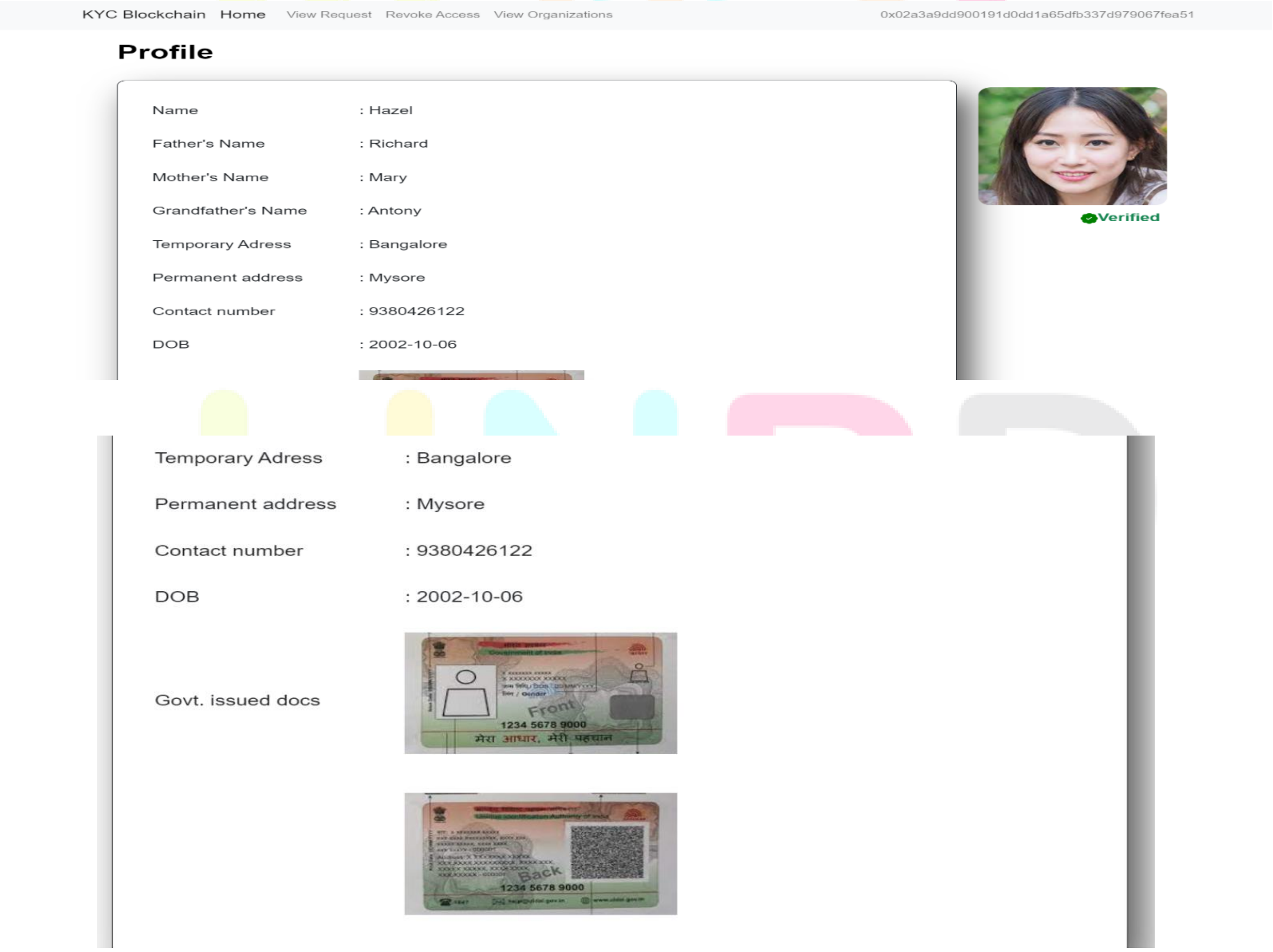
Organization Details

Organization Name : Canara bank

Organization Eth Address : 0xaB8DeCF0D50Fb3c4BacB6D278beE597148981459

fig 4. organization page

CUSTOMER PAGE:



KYC Blockchain Home View Request Revoke Access View Organizations
0x02a3a9dd900191d0dd1a65dfb337d979067fea51
Verified

Profile

Name : Hazel

Father's Name : Richard

Mother's Name : Mary

Grandfather's Name : Antony

Temporary Adress : Bangalore

Permanent address : Mysore

Contact number : 9380426122

DOB : 2002-10-06

Temporary Adress : Bangalore

Permanent address : Mysore

Contact number : 9380426122

DOB : 2002-10-06

Govt. issued docs

Front
1234 5678 9000
मेरा आधार, मेरी पहचान
Back
1234 5678 9000

fig 5. customer page

V. REFERENCES

1. Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, Qiaoyan Wen, (June 2020), A Survey on the Security of Blockchain Systems

2. Diksha Malhotra, Poonam Saini & Awadhesh Kumar Singh ,(25 August 2021) , How Blockchain Can Automate KYC: Systematic Review

3. Somchart Fugkeaw, (05 May 2022), Enabling Trust and Privacy-Preserving e-KYC System Using Blockchain

4. Pradnya Patil, M. Sangeetha, (2022), Blockchain-based Decentralized KYC Verification Framework for Banks

5. Vincent Schlatt, Johannes Sedlmeir, Simon Feulner, Nils Urbach, (November 2022), Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity