KYC VERIFICATION USING BLOCKCHAIN

SHAIK ABDUL SHAKIR
SOCS, Presidency University

SOMALA NITHYA SAI
SOCS, Presidency University

SHAIK AKBAR BASHA
SOCS, Presidency University

KUSUM HARI TEJA REDDY
SOCS, Presidency University

MAJJARI CHANDRA SEKHAR
SOCS, Presidency University

Dr. Pravinth Raja,
Associate Professor,
School of Computer Science and Engineering,
Presidency University.

ABSTRACT

KYC (Know Your Customer) verification is essential for regulatory compliance, but traditional methods are often inefficient, costly, and prone to data duplication. This study introduces a blockchain-based decentralized system to automate KYC processes, including document submission, validation, and approval, using smart contracts. Customers can securely upload documents through an intuitive interface, while administrators review and process the data directly on the blockchain. The decentralized structure ensures tamper-proof, transparent, and auditable data storage, minimizing reliance on intermediaries and reducing delays. Advanced cryptographic techniques, such as Zero-Knowledge Proofs (ZKPs), protect sensitive information during verification, while Secure Hash Algorithm (SHA)-based encryption ensures data confidentiality and integrity. This approach streamlines KYC workflows, enhances security, and reduces operational costs, offering a scalable and privacy-focused solution for regulatory compliance.

KEYWORDS

Decentralized Application, Smart Contracts, User Onboarding, KYC Verification, Blockchain Technology, Security.

INTRODUCTION

The widespread adoption of digital technologies has created a pressing need for effective and reliable identity verification across various industries. Traditional Know Your Customer (KYC) methods, often relying on manual and centralized processes, face numerous challenges such as lengthy delays, high costs, and vulnerability to errors or fraud. Moreover, centralized systems that store sensitive customer data in a single location are at greater risk of breaches. As businesses strive to meet regulatory requirements, the demand for innovative, secure, and efficient solutions that also give users control over their data has grown significantly.

This research introduces a blockchain-based decentralized application (DApp) to streamline and secure KYC verification processes. By utilizing smart contracts, the DApp automates key tasks such as document submission, verification, and approval, ensuring tamper-proof workflows. Blockchain technology provides a transparent and immutable record, reducing dependency on intermediaries and addressing inefficiencies. Cryptographic techniques like Secure Hash Algorithms (SHA) and Zero-Knowledge Proofs (ZKPs) safeguard sensitive data by allowing identity verification without exposing personal details. The system's intuitive interface simplifies document management for users, while its multi-chain architecture supports scalability and high transaction volumes. This decentralized solution addresses the flaws of traditional systems, fostering trust by emphasizing data security and transparency. By reducing processing times and costs, it offers a modern, adaptable framework for identity verification that aligns with evolving regulations and technological advancements.

MOTIVATION

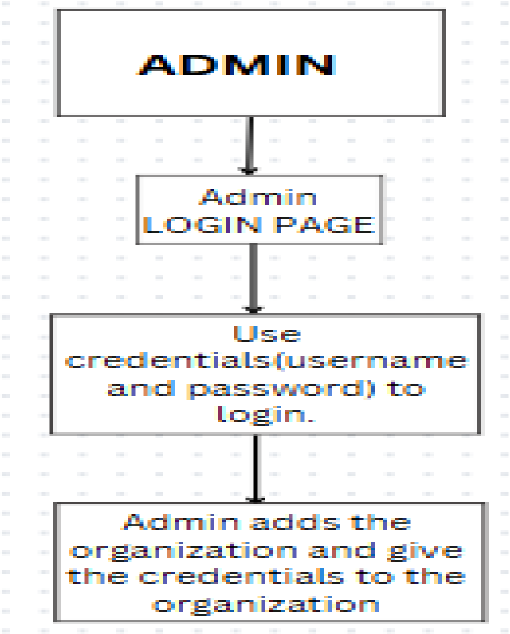
The rising need for secure and efficient identity verification systems, alongside the expanding adoption of blockchain technology, serves as a key driver for this research. Traditional KYC (Know Your Customer) processes often suffer from inefficiencies, high costs, and vulnerability to data breaches. By leveraging the capabilities of smart contracts, this study proposes the development of a decentralized application (DApp) to overcome these challenges. The DApp aims to streamline KYC processes by offering improved security, faster processing times, and enhanced transparency, all while reducing operational costs. Moreover, the decentralized structure ensures robust data privacy and immutability, empowering users with greater control over their personal information. This approach aligns with the growing emphasis on trustless systems in modern technology, eliminating the need for intermediaries. The use of blockchain also facilitates tamper-proof data storage, creating a verifiable and transparent audit trail. As a result, the proposed solution has the potential to revolutionize identity verification and set a new standard in data security and efficiency.

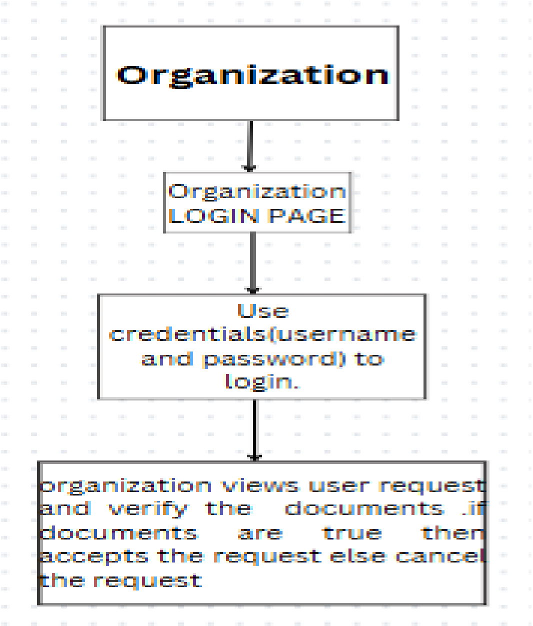
OBJECTIVES

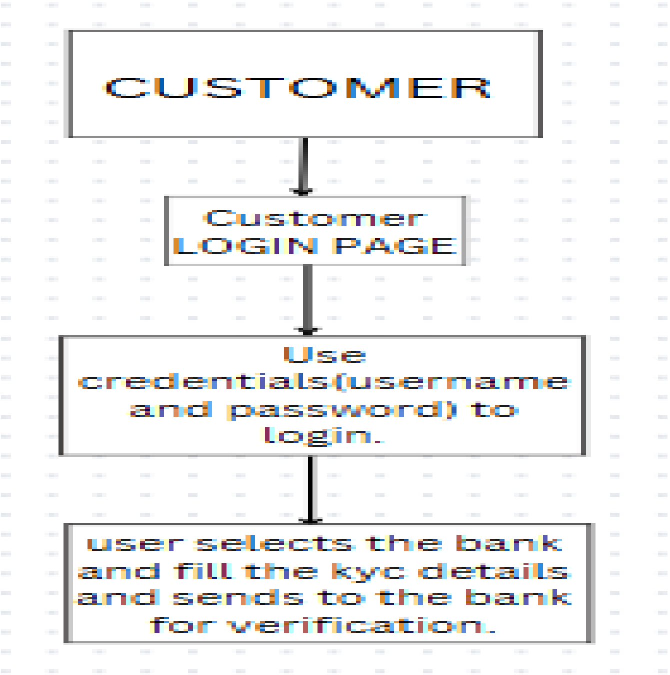
Based on the observations and research gaps in the current KYC verification process, the following objectives have been formulated:

1. To develop a blockchain-based KYC system for secure and efficient customer verification.
2. To ensure decentralized storage and immutable records of KYC data to enhance trust and transparency.
3. To streamline the KYC process by enabling data sharing across authorized financial institutions while maintaining privacy.
4. To utilize cryptographic techniques for secure access control and verification of customer credentials.
5. To reduce redundancy in KYC verification by creating a single source of truth accessible to multiple entities.
6. To provide real-time verification with faster processing times compared to traditional systems.

METHODOLOGY


ADMIN
Admin LOGIN PAGE
Use credentials(username and password) to login.
Admin adds the organization and give the credentials to the organization


Organization
Organization LOGIN PAGE
Use credentials(username and password) to login.
organization views user request and verify the documents .if documents are true then accepts the request else cancel the request


CUSTOMER
Customer LOGIN PAGE
Use credentials(username and password) to login.
user selects the bank and fill the kyc details and sends to the bank for verification.

The three images represent flowcharts depicting the login and credential verification processes for different entities (Admin, Customer, and Organization) in a KYC system:

1. Admin Flowchart
    - Start: Admin access begins.
    - Admin Login Page: Admin navigates to the login page.
    - Use Credentials: The admin uses a username and password to log in.
    - Organization Management:
        - The admin adds an organization and view organizations added.
        - The admin provides login credentials to the organization for future use.
2. Customer Flowchart
    - Start: Customer access begins.
    - Customer Login Page: The customer navigates to the login page.
    - Use Credentials: The customer uses their username and password to log in.
    - Bank and KYC Submission:
        - The customer selects a bank.
        - Fills in KYC details.
        - Submits the details to the bank for verification.
3. Organization Flowchart
    - Start: Organization access begins.
    - Organization Login Page: The organization navigates to the login page.
    - Use Credentials: The organization uses a username and password to log in.
    - View and Verify Requests:
        - The organization views customer KYC requests.
        - Verifies the submitted documents.
        - If documents are valid, the organization accepts the request.
        - If invalid, the organization rejects or cancels the request.

The KYC verification system involves three primary stakeholders: Admin, Customer, and Organization, each with distinct roles and processes. The Admin begins the process by accessing the Admin login page, logging in with valid credentials, and adding organizations to the system, providing them with the required credentials. Next, the Customer accesses the Customer login page, logs in using their credentials, selects the bank, fills in their KYC details, and submits the information for verification. The Organization then logs in through the Organization login page using their credentials, views incoming user requests, and verifies the submitted documents. If the documents are valid, the request is accepted; otherwise, it is rejected or canceled. This step-by-step methodology ensures a structured flow of operations, enabling secure login-based access, data submission, and document verification to maintain a transparent and efficient KYC process.

EXCEPTED OUTCOMES

Streamlined User Authentication

- Based on the flowcharts, all stakeholders (Admin, Customer, and Organization) will securely log in using credentials (username and password) to access the system, ensuring authenticated access to KYC functionalities.

 Efficient Organization Onboarding

- The **Admin** will successfully add organizations to the system and provide them with login credentials, enabling smooth onboarding of trusted entities into the blockchain-based KYC ecosystem.

 Simplified Customer KYC Submission

- Customers will log in, select a bank, fill in KYC details, and submit them for verification. This ensures a user-friendly and structured process for KYC document submission.

 Seamless Document Verification by Organizations

- Organizations will view customer KYC requests, verify submitted documents, and decide on acceptance or rejection based on authenticity. This streamlines the verification process and reduces manual intervention.

 Improved Data Transparency and Accessibility

- Using blockchain, verified KYC data will be immutable and accessible only to authorized organizations upon user consent. This aligns with the flowcharts where credentials play a role in managing access.

 Faster KYC Processing

- By following a systematic process as shown in the flowcharts, the system will reduce delays and ensure that users receive quick feedback regarding the acceptance or rejection of their KYC verification.

 Secure and Tamper-Proof System

- Storing KYC data on the blockchain will ensure it cannot be tampered with. Admins, customers, and organizations will interact through secure logins, as outlined in the flowcharts.

 User-Centric Workflow

- The workflows demonstrated in the images ensure clear responsibilities:
  - **Admins** manage organizations.
  - **Customers** submit their KYC details.
  - **Organizations** verify and process requests.

CONCLUSION

In conclusion, this research highlights the transformative potential of blockchain technology in addressing the limitations of traditional KYC verification processes. By leveraging smart contracts within a decentralized application (DApp), the proposed system enhances efficiency, security, and transparency in user onboarding and KYC verification. The elimination of intermediaries reduces processing time and operational complexities, while the immutable nature of blockchain ensures data integrity and trustworthiness. This approach not only streamlines the verification process but also aligns with modern demands for secure and user-centric solutions in identity verification. The findings underscore the viability of blockchain-powered DApps as a robust alternative to conventional systems, paving the way for further advancements in secure and decentralized identity management.

COMPARISON

Survey Paper Abstract:

Examines the use of centralized frameworks and manual processes for KYC (Know Your Customer) verification. These systems rely heavily on human intervention, leading to higher costs, slower operations, and increased vulnerability to data breaches. Traditional KYC systems often lack efficiency, requiring customers to undergo repeated verifications across various institutions, thereby introducing redundancy and user inconvenience.

Our Project Abstract:

Explores the adoption of a blockchain-driven KYC system to address the limitations of conventional approaches. By utilizing decentralized ledger technology, the proposed solution offers enhanced security, immutability, and transparency in KYC processes. Unlike traditional systems, this blockchain-based approach eliminates repetitive verifications by maintaining a shared, tamper-proof ledger accessible to authorized organizations. The system minimizes costs, reduces processing times, and enhances user experience by streamlining verification procedures.

Survey Paper Abstract:

Analyzes KYC solutions where customer data is stored on centralized servers, presenting risks of single points of failure and susceptibility to cyberattacks. While some systems integrate automated checks, their lack of interoperability restricts the reuse of KYC information across multiple institutions, resulting in inefficiencies and non-scalable implementations.

Our Project Abstract:

Leverages blockchain technology to implement cryptographically secured smart contracts, ensuring privacy, data integrity, and security. The system empowers users by giving them control over their KYC data, enabling selective access to authorized entities on-demand. With interoperability as a core feature, this approach fosters seamless collaboration among institutions while adhering to regulatory standards. The solution is designed to be scalable, efficient, and resilient to the challenges faced by centralized KYC models.

Survey Paper Abstract:

Investigates traditional KYC models that depend on third-party intermediaries for verification and data management. These models often suffer from long processing times, higher costs, and a lack of real-time updates. Furthermore, the dependence on intermediaries introduces security vulnerabilities and limits direct user control over sensitive information.

Our Project Abstract:

Proposes a blockchain-powered KYC framework that eliminates the need for intermediaries by automating processes through smart contracts. The decentralized system facilitates real-time data sharing and verification, significantly improving efficiency and reducing costs. Customers maintain ownership of their data, ensuring security and privacy while providing authorized institutions with controlled access. This approach not only enhances trust and reliability but also addresses the inefficiencies inherent in traditional KYC models.

REFERENCES

Esraa Elgamal; Walaa Medhat; Mohamed Abd Elfatah; Nashwa Abdelbaki; Blockchain Application on Big Data Security; 26-26 January 2023.

Mohamed Fartitchou; Khalid El Makkaoui; Nabil Kannouf; Zakaria El Allali; Security on Blockchain Technology; 04-06 September 2020.

S. Manimurgan; T. Anitha; G. Divya; G. Charlyn Pushpa Latha; S. Mathupriya; A Survey on Blockchain Technology for Network Security Applications; 25-27 January 2022.

Austin Draper; Aryan Familrouhani; Devin Cao; Tevisophea Heng; Wenlin Han; Security Applications and Challenges in Blockchain; 11-13 January 2019.

Labbe, A., “Companies bank on blockchain bonds to cut costs, time,” International Financial Law Review, Sept. 2017

Karl Flinders, “Emirates Islamic uses blockchain to reduce cheque fraud,” available at: https://www.computerweekly.com/news/450421051/EmiratesIslamic-uses-blockchain-to-reduce-cheque-fraud, Jun 21, 2017.

Wilson, D., and Ateniese, G., “From Pretty Good To Great: Enhancing PGP using Bitcoin and the Blockchain,” Network and System Security, vol. 9408, pp. 368-375, Nov. 2015.

Sivakumar P., and Kunwar Singh, “Privacy based decentralized Public Key Infrastructure (PKI) implementation using Smart contract in Blockchain,” technical report.

Abdullah Al Mamun; Sheikh Riad Hasan; Md Salahuddin Bhuiyan; M. Shamim Kaiser; Mohammad Abu Yousuf.” Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology”.

N. Sundareswaran; S. Sasirekha; I. Joe Louis Paul; S. Balakrishnan; G. Swaminathan,” Optimised KYC Blockchain System”.