International Journal of Engineering Research and Science & Technology

BLOCKCHAIN-BASED KYC MODEL FOR CREDIT ALLOCATION IN BANKING

E. MOUNIKA REDDY[1], SUKKA ANJALI [2], SHAIK NAVEED[3], VIROTHI TAGOOR BABU[4], VAGAVATH BHANU PREETHAM[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— The implementation of the Know Your Customer (KYC) strategy by banks within the financial sector enhances the operational efficiency of such establishments. The data gathered from the client during the KYC procedure may be applied to deter possible fraudulent activities, money laundering, and other criminal undertakings. The majority of financial institutions implement their own KYC procedures. Furthermore, a centralized system permits collaboration and operation execution by multiple financial institutions. Aside from these two scenarios, KYC processes can also be executed via a blockchain-based system. The blockchain's decentralized network would be highly transparent, facilitating the validation and verification of customer data in real-time for all relevant stakeholders. In addition, the immutability and cryptography of the blockchain ensure that client information is secure and immutable, thereby eradicating the risk of data breaches. Blockchain-based KYC can further improve the client experience by eliminating the requirement for redundant paperwork and document submissions. After banks grant consumers transactions, a blockchain-based KYC system is proposed in this study to collect limit, risk, and collateral information from them. The approach built upon Ethereum grants financial institutions the ability to read and write financial data on the blockchain network. This KYC method establishes a transparent, dynamic, and expeditious framework among financial institutions. In addition, solutions are discussed for the Sybil attack, one of the most severe problems in such networks.

Index Terms – Blockchain-Based KYC, Credit Allocation, Banking, Blockchain Technology, Smart Contracts, Identity Verification, Fraud Prevention, FinTech, Secure Transactions, Digital Banking.

I. INTRODUCTION

Blockchain is a type of distributed record keeping in a decentralized network by many nodes. Each of these nodes maintains a copy of the entire blockchain of records. Due to its distinctive features such as decentralization, transparency, robustness, auditability and security, blockchain appears to affect many traditional ways of doing business. Although blockchain is an old topic, its awareness has increased with Bitcoin. Bitcoin's technical document is the article titled ''Bitcoin: A Peer-to-Peer Electronic Cash System'' written in 2008 by a person or group named Satoshi Nakamoto. The article proposes the transfer of digital assets using blockchain technology without using a financial intermediary. The article explains in detail how the double spending problem, one of the most serious problems of electronic money transfers, is solved when making these transfers. The infrastructure of this transfer system is built on blockchain technology, which provides a distributed ledger structure. Each network participant is considered a node in the blockchain, and transactions made by nodes are linked together in blocks. Since Satoshi Nakamoto first published his Bitcoin whitepaper in 2008, three generations of blockchains have been adopted. Blockchain 1.0 is used for cryptocurrency transactions, Blockchain 2.0 for financial applications, and Blockchain 3.0 for applications in areas other than finance, such as government, healthcare, and science. In the financial sector, blockchain is used in a variety of ways. The most essential of them are cryptocurrency exchanges, KYC, payment systems, sukuk, non-fungible tokens (NFTs), and crowdfunding. KYC is typically a process carried out individually by banks. It is also possible for banks to share information and conduct the transaction centrally. Apart from this, a KYC procedure can be carried out using blockchain. The use of blockchain technology in the KYC process benefits consumer risk management by making it faster, more transparent, and decentralized. Following the use of a loan, a bank customer is obliged to make periodical loan payments to the bank. In the process, banks should measure their risks by sharing information with other banks on limits, risks and collateral. Banks can more quickly determine the risks related to their customers if they have this information. Conventional

credit assessment relies on centralized credit bureaus. These entities gather customer financial information from banks and subsequently monetize it by selling it back to financial institutions. However, this approach raises concerns regarding data ownership and security, as credit bureaus possess the ability to manipulate the information. Furthermore, the data retrieval process is often delayed, as it typically occurs on an end-of-day basis. In contrast, a blockchain-based model fosters a decentralized environment where all participating banks hold identical copies of customer financial data. This shared ledger enables immediate data access for authorized institutions, eliminating the need for a centralized intermediary and associated fees. Decentralized blockchain technology has the potential to significantly enhance the overall efficiency of KYC processes. This can be achieved through several mechanisms: improved processing speed, minimized onboarding time for customers, reduced risk of fraud and money laundering, and a decrease in total costs incurred by financial institutions. In this study, the method of sharing the limit, risk and collateral information of bank customers using credit between banks using blockchain is explained. Using the Ethereum network, a blockchainbased system was established with the help of a smart contract in the Solidity language. After a bank provides a loan to its customer, it enters the customer's limit, risk and collateral information into the system. At the same time, if that customer has used a loan from another bank, the bank also accesses the limit, risk and collateral information entered by that bank. Since this study is designed on a private blockchain network, it does not pose a problem with the Sybil attack. The authors confirm contribution to the paper as follows: study conception and design: B. Karadag, A.H.Zaim, A. Akbulut; model creation: B. Karadag, A. Akbulut; analysis and interpretation of results: B. Karadag, A.H.Zaim, A. Akbulut; draft manuscript preparation: B. Karadag, A. Akbulut. All authors reviewed the results and approved the final version of the manuscript.

II. RELATED WORK

A. A review of blockchain approaches for KYC

The traditional Know Your Customer (KYC) procedure used by banks is deemed unreliable and costly. Therefore, the adoption of emerging technologies is essential for banking firms' future prospects. One such technology that has gained widespread acceptance is Blockchain, which is known for

its reliability and security across various fields. This study aims to investigate how the implementation of Blockchain technology can modify the existing banking business, particularly the KYC document verification process, by storing and monitoring of information. The current need for an optimized KYC system is paramount; one that is coupled with a secure and trustworthy technology like Blockchain that can withstand fraudulent activities while also overcoming scalability and privacy challenges. The article analyzes previous relevant works, which highlight how the implementation of Blockchain technology eliminates the need for intermediaries, thereby reducing the possibility of malicious activities and errors that may occur when there are multiple manual tasks involved.

B. *Bank records storage system through blockchain*

This research puts forth a system that utilizes the integration of blockchain, a database for storage, and cryptography to preserve the confidentiality and security of bank records. The blockchain ensures the protection and dependability of data storage through its use, while smart contracts regulate the way the data is stored and shared. The original bank records are kept in a secured, encrypted format on a separate database, with only their hash values recorded on the blockchain. To further secure the data, the off-chain records are frequently connected with the hash information on the blockchain. The utilization of cryptography aids in the encryption of documents and the digital signing of messages. The system has a WebApp interface that enables parties involved in the transaction to communicate in a decentralized manner.

C. *Sybil in the haystack: A comprehensive review of blockchain consensus mechanisms in search of strong Sybil attack resistance*

Consensus algorithms are applied in the context of distributed computer systems to improve their fault tolerance. The explosive development of distributed ledger technology following the proposal of “Bitcoin” led to a sharp increase in research activity in this area. Specifically, public and permissionless networks require robust leader selection strategies resistant to Sybil attacks in which malicious attackers present bogus identities to induce byzantine faults. Our goal is to analyse the entire breadth of works in this area systematically, thereby uncovering trends and research directions regarding Sybil attack resistance in today’s blockchain

systems to benefit the designs of the future. Through a systematic literature review, we condense an immense set of research records (N = 21,799) to a relevant subset (N = 483). We categorise these mechanisms by their Sybil attack resistance characteristics, leader selection methodology, and incentive scheme. Mechanisms with strong Sybil attack resistance commonly adopt the principles underlying "Proof-of-Work" or "Proof-of-Stake" while mechanisms with limited resistance often use reputation systems or physical world linking. We find that only a few fundamental paradigms exist that can resist Sybil attacks in a permissionless setting but discover numerous innovative mechanisms that can deliver weaker protection in system scenarios with smaller attack surfaces.

III. PROPOSED METHODOLOGY

KYC helps in identifying and preventing fraudulent activities. By knowing who their customers are, banks can better detect suspicious transactions and patterns that may indicate fraud.

Many countries have laws and regulations requiring financial institutions to implement KYC procedures. Compliance with these regulations helps banks avoid legal penalties and ensures that they are operating within the law.

All actions related to KYC data are recorded on the blockchain, enhancing transparency and accountability.

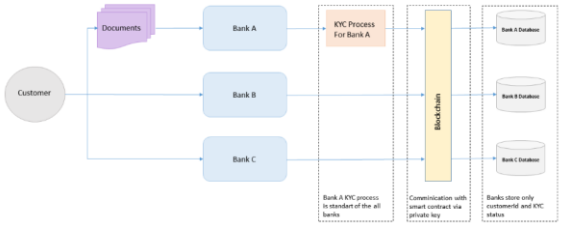
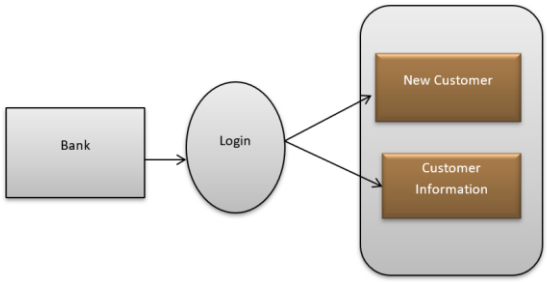


Fig. 1: System Overview

1. Bank

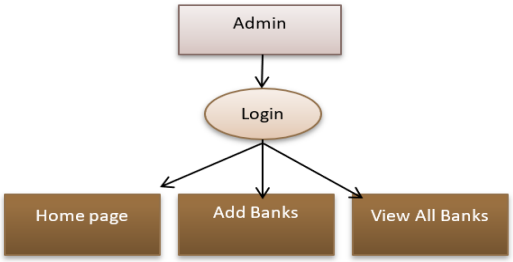
Banks play a vital role in the financial system by providing essential services that facilitate economic activity and personal financial management. They offer a secure place for individuals and businesses to deposit and manage their money, ensuring the safekeeping of funds against theft or loss.



2. Admin

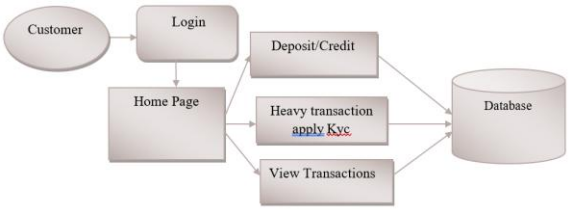
This is the third module in our project is Admin. Here admin will login with his password and Id who has created by the bc

operator. After admin login directely will navigate into admin home page. The purpose of an administrator is to oversee and manage the operations and functionality of an organization, system, or project. Administrators are responsible for coordinating tasks, enforcing policies, and ensuring that processes run smoothly and efficiently.



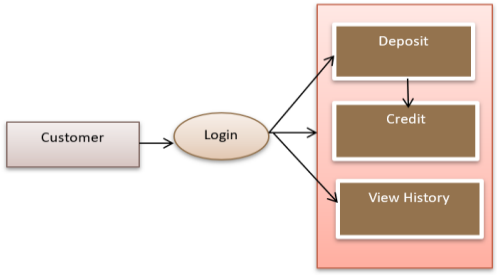
3. Customer

This is the fourth module in our project is Customer. Customers must provide accurate, complete, and up-to-date personal information, address, as requested by the bank. They are also required to submit the necessary documentation promptly and update their details if there are any changes, such as a new address or a name change. Customer bank transactions encompass a range of financial activities performed by account holders through their banking institution. These transactions include deposits, where customers add funds to their accounts; withdrawals, where they remove money; transfers, where they move funds between accounts or to other individuals or institutions. Each transaction is recorded and monitored by the bank to ensure accuracy and to maintain a comprehensive account history.



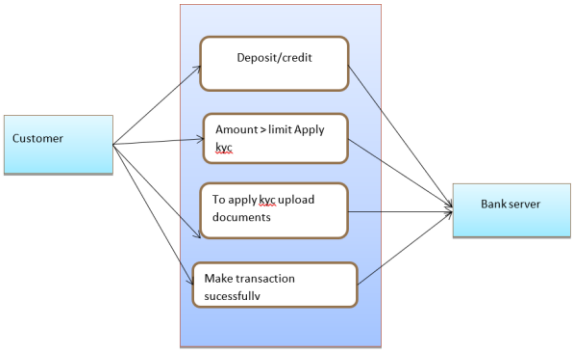
4. Transactions

This is the Fifth module in our project is Transactions. Credit and deposit transactions are fundamental activities in banking where customers interact with their accounts. A credit occurs when funds are added to a customer's account, such as through a paycheck deposit, loan disbursement, or a transfer from another account. Deposits, on the other hand, involve customers placing money into their accounts, which can be done through various methods including cash deposits, checks, or electronic transfers. Banks record these transactions meticulously to ensure account balances are accurately updated and to provide customers with a clear and detailed account of their financial activity.



5. KYC

Know Your Customer (KYC) is a crucial process employed by financial institutions to verify the identity of their clients and assess potential risks of illegal activities, such as money laundering or fraud. Through KYC procedures, banks and other financial entities collect and analyze personal information from customers, including identity documents, proof of address, and financial history.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrated that the integration of Blockchain Technology enabled secure and tamper-resistant storage of customer identity information while significantly reducing the time required for KYC verification and credit approval processes.

The analysis showed that the decentralized architecture improved transparency, traceability, and trust among participating financial institutions while minimizing duplication of KYC procedures. Furthermore, the implementation of smart contract-based credit evaluation mechanisms reduced operational costs and enhanced resistance against identity fraud and data manipulation attacks.

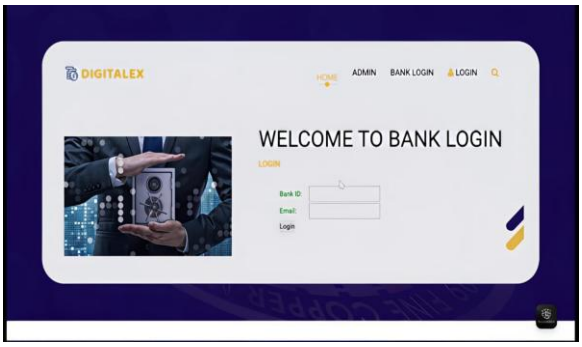


Fig. 2: Bank Login

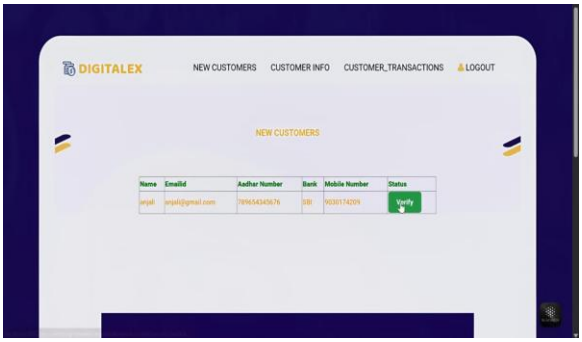


Fig. 3: Verify Customers

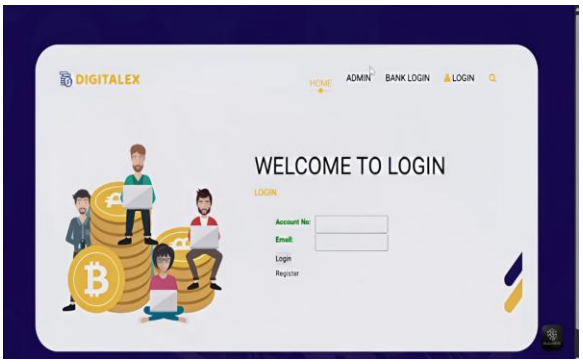


Fig. 4: Login

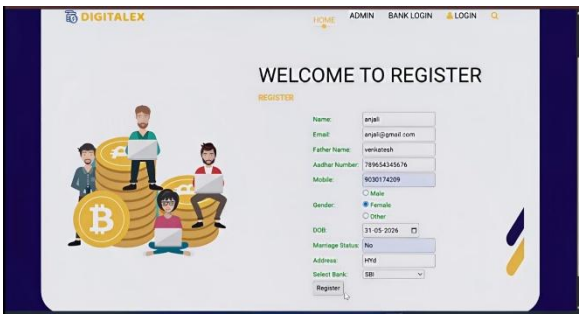


Fig. 5: Registration

V. CONCLUSION

The blockchain-based KYC model was designed considering the private Ethereum network and PoS consensus mechanism. In this way, blockchain technology offers a transformative solution to the shortcomings of traditional KYC in banking. A shared, immutable ledger streamlines onboarding, bolsters data security, and enables real-time risk assessment. Regulatory hurdles persist, but the potential for enhanced efficiency, collaboration, and risk management within a secure and transparent framework is undeniable. As blockchain matures and regulations evolve, it has the potential to revolutionize KYC, ushering in a new era for secure and efficient customer identification in banking.

REFERENCES

[1] V. L. Lemieux, ‘‘Trusting records: Is blockchain technology the answer?’’ Records Manage. J., vol. 26, no. 2, pp. 110–139, Jul. 2016.

[2] W. Viriyasitavat and D. Hoonsopon, ‘‘Blockchain characteristics and consensus in modern business processes,’’ J. Ind. Inf. Integr., vol. 13, pp. 32–39, Mar. 2019.

[3] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: Apr. 18, 2023. [Online]. Available: https://bitcoin. org/bitcoin.pdf

[4] S. Perera, S. Nanayakkara, M. N. N. Rodrigo, S. Senaratne, and R. Weinand, ‘‘Blockchain technology: Is it hype or real in the construction industry,’’ J. Ind. Inf. Integr., vol. 17, pp. 1–20, Jan. 2020.

[5] B. Karadag, A. Akbulut, and A. H. Zaim, ‘‘A review on blockchain applications in fintech ecosystem,’’ in Proc. Int. Conf. Adv. Creative Netw. Intell. Syst.

(ICACNIS), Nov. 2022, pp. 1–5, doi: 10.1109/ICACNIS57039.2022.10054910.

[6] Ethereum. (2023). Ethereum Whitepaper.

AUTHORS Profile



Mrs. E. MOUNIKA REDDY has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 8 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Ms. SUKKA ANJALI pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. SHAIK NAVEED pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. VIROTHI TAGOOR BABU pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. VAGAVATH BHANU PREETHAM pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.