International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

A Secure And Transparent KYC And Credit Scoring Framework Using Blockchain

[1]Ajay Sharma,[2]Manchuri Aryan Kumar, [3] Kosigi Krishna Chaithanya, [4]Kalugotla Hemanth,[5] D.Sai Ranjith Kumar
[1] Assistant Professor, Department of Computer Science & Engineering, Dr. K.V. Subba Reddy Institute of Technology
[2,3,4 ,5] B. Tech Students, Department of Computer Science & Engineering, Dr. K.V. Subba Reddy Institute of Technology

ABSTRACT

Know Your Customer (KYC) verification and credit scoring are critical processes in the banking and financial sectors to ensure regulatory compliance, prevent fraud, and assess customer creditworthiness. However, traditional KYC and credit scoring systems are centralized, repetitive, time-consuming, and vulnerable to data breaches. Customers are often required to submit the same documents multiple times to different financial institutions, leading to inefficiencies and poor user experience. Moreover, conventional credit scoring models lack transparency and fail to provide trust in decision-making. This project proposes a secure and transparent KYC and Credit Scoring framework using Blockchain technology. Blockchain provides a decentralized, tamper-proof, and auditable ledger for storing verified KYC records and credit-related transactions. Smart contracts automate identity verification and credit score updates while ensuring data privacy and user consent. By integrating blockchain with analytics-based credit scoring models, the proposed system enhances security, transparency, trust, and operational efficiency in financial services.

Keywords: Blockchain, Know Your Customer (KYC), Credit Scoring, Distributed Ledger Technology (DLT), Smart Contracts, Decentralized Identity, Financial Security, Data Privacy, Cryptographic Hashing, Financial Technology (FinTech), Risk Assessment, Transparency.

I. INTRODUCTION

The financial industry is undergoing rapid digital transformation, yet identity verification and credit assessment remain largely inefficient and opaque. KYC processes require customers to repeatedly submit sensitive documents, while credit scoring models often function as black boxes. Blockchain technology, with its decentralized architecture, immutability, and cryptographic security, provides a novel approach to managing digital identities and credit information.

A blockchain-based KYC and credit scoring system enables secure data sharing among authorized entities without relying on a central authority. Smart contracts automate verification workflows and ensure compliance with regulatory standards. This project focuses on leveraging blockchain to create a trustworthy, efficient, and privacy-preserving KYC and credit scoring ecosystem.

II. LITERATURE SURVEY

1. Title: Blockchain-Based Know Your Customer (KYC) Systems

Author: A. Zyskind and O. Nathan

Description:

This study explores blockchain-based identity management systems and demonstrates how decentralized architectures enhance privacy and security in KYC processes.

2. Title: Decentralized Identity Management Using Blockchain

Author: C. Allen

Description:

The paper introduces decentralized identity concepts and explains how blockchain can provide user-controlled digital identities.

3. Title: Credit Scoring Models in Financial Services

Author: D. J. Hand and W. E. Henley

Description:

This research reviews traditional and modern credit scoring techniques and highlights the need for transparency and explainability.

4. Title: Smart Contracts for Secure Financial Applications

Author: N. Szabo

Description:

The author discusses the role of smart contracts in automating financial processes and enforcing trust without intermediaries.

5. Title: Blockchain Technology in Banking and Finance

Author: M. Crosby et al.

Description:

This paper analyzes blockchain applications in banking, emphasizing secure data sharing, fraud prevention, and regulatory compliance.

III. EXISTING SYSTEM

In the existing system, KYC and credit scoring are handled independently by each bank or financial institution using centralized databases. KYC verification involves manual document checks, third-party verification services, and repeated onboarding processes. Credit scoring is typically performed using proprietary models based on limited financial data. These systems suffer from poor interoperability, lack of transparency, and high vulnerability to cyberattacks.

IV. PROPOSED SYSTEM

The proposed system introduces a blockchain-based decentralized framework for managing KYC and credit scoring. Verified KYC data is securely stored on the blockchain in encrypted form, accessible only with user consent. Smart contracts automate identity verification, approval workflows, and credit score updates. Credit scoring models utilize verified transactional and behavioral data, ensuring accuracy and transparency. This framework enables seamless data sharing among financial institutions while maintaining security and privacy.

V. SYSTEM ARCHITECTURE

The proposed Secure and Transparent KYC and Credit Scoring Framework Using Blockchain is designed as a multi-layered, distributed architecture that ensures data privacy, transparency, immutability, and trust among financial institutions, users, and regulatory bodies. The architecture is primarily divided into five major layers: User Layer, Application Layer, Blockchain Layer, Off-Chain Storage Layer, and Regulatory & Analytics Layer. Each layer performs specific tasks while collectively maintaining a secure and tamper-proof ecosystem for digital identity verification and credit evaluation.

At the User Layer, customers, banks, financial institutions, and regulatory authorities interact with the system through secure web or mobile interfaces. Customers initiate KYC registration by submitting identity documents such as Aadhaar, PAN, passport, income statements, and transaction history. These documents are encrypted on the client side before transmission. Financial institutions access verified KYC records and credit scores through authenticated APIs, ensuring that only authorized entities can view sensitive information. Multi-factor authentication and digital signatures are used to strengthen identity validation and prevent unauthorized access.

The Application Layer acts as the middleware that processes requests, performs validation checks, and communicates with the blockchain network. This layer contains KYC validation modules, credit scoring engines, encryption services, and API gateways. Once a user submits documents, the system verifies authenticity using AI-based document verification and cross-checks with government or financial databases. After validation, the system generates a unique digital identity and calculates preliminary credit metrics based on historical transaction data, repayment behavior, and risk indicators. The processed data is then hashed and prepared for blockchain storage.

The Blockchain Layer is the core component of the architecture. It consists of a permissioned blockchain network where participating banks and authorized institutions function as nodes. Smart contracts automate KYC verification approval, access control, and credit score updates. When a user's KYC is verified, a cryptographic hash of the verified data is stored on the blockchain ledger. This ensures immutability and prevents tampering. Any update in user information or credit history triggers a new transaction recorded on the blockchain, creating a transparent audit trail. Since the blockchain is decentralized, no single entity can manipulate records, thereby enhancing trust among stakeholders. The Off-Chain Storage Layer stores large documents

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

and sensitive personal data securely in encrypted databases or distributed storage systems such as IPFS or secure cloud storage. Only the cryptographic hash of the data is stored on-chain, while the actual files remain off-chain to improve scalability and reduce storage costs. Access to off-chain data is controlled through smart contracts and secure key management systems. This hybrid storage approach balances efficiency, privacy, and transparency while complying with data protection regulations.

The Credit Scoring Engine, integrated within the analytics module, continuously evaluates user financial behavior. It collects transaction records, loan repayment history, digital payments, and alternative financial data. Machine learning algorithms analyze these features to generate dynamic credit scores. Every time a score is updated, the result is recorded on the blockchain, ensuring transparency and preventing fraudulent manipulation of credit ratings. Financial institutions can instantly access real-time credit scores without repeating the KYC process, thereby reducing operational costs and onboarding time.

The Regulatory & Monitoring Layer provides oversight capabilities for compliance authorities. Regulators can audit transactions, verify KYC compliance, and monitor suspicious activities in real time through read-only blockchain access. Since all transactions are time-stamped and immutable, regulatory reporting becomes more accurate and efficient. Machine learning algorithms analyze these features to generate dynamic credit scores.This layer enhances accountability and reduces the risk of financial fraud, money laundering, and identity theft. Overall, the architecture ensures security through encryption and hashing, transparency through distributed ledger technology, automation through smart contracts, and efficiency through AI-driven credit scoring. Machine learning algorithms analyze these features to generate dynamic credit scores. Machine learning algorithms analyze these features to generate dynamic credit scores. By integrating blockchain with intelligent analytics, the system eliminates redundant KYC procedures, reduces fraud, enhances trust among institutions, and provides a secure digital identity framework for financial ecosystems.

Fig 5.1: Structure of the Proposed System

The image illustrates a comparative view between the traditional centralized KYC system and a blockchain-based KYC framework, highlighting differences in cost, effort, efficiency, and transparency. On the left side, the centralized database model shows a customer submitting KYC documents to a bank, which then forwards the documents to a centralized intermediary that stores the data. This process involves significant data storage and security costs because sensitive customer information is maintained in a single centralized repository, making it vulnerable to breaches and cyberattacks. Additionally, when other financial institutions require the same customer's KYC details, they must request verification from the intermediary, leading to repetitive KYC checks, duplicated efforts, increased operational costs, and longer processing times. The dependency on intermediaries not only increases administrative overhead but also creates delays and inefficiencies due to manual verification and compliance procedures.

In contrast, the right side of the image demonstrates how blockchain technology streamlines and optimizes this process. Here, the customer directly uploads KYC data to a blockchain network, where it is securely recorded using cryptographic mechanisms. Once verified by a bank, the validated KYC record becomes accessible to other authorized institutions on the blockchain, eliminating the need for repeated verification processes. Since the data is distributed and tamper-resistant, there is reduced reliance on centralized storage systems and intermediaries, which significantly lowers costs associated with data security, storage, and compliance management. The blockchain ensures

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

transparency because all participating institutions can trust the shared ledger without needing to independently revalidate the information. Once verified by a bank, the validated KYC record becomes accessible to other authorized institutions on the blockchain, eliminating the need for repeated verification processes. Once verified by a bank, the validated KYC record becomes accessible to other authorized institutions on the blockchain, eliminating the need for repeated verification processes. As a result, the framework saves time, reduces duplication of effort, enhances trust among financial entities, and improves overall operational efficiency while maintaining strong security and integrity of customer data.

VI. IMPLEMENTATION

Fig 6.1: KYC Dashboard

Fig 6.2: KYC Verification

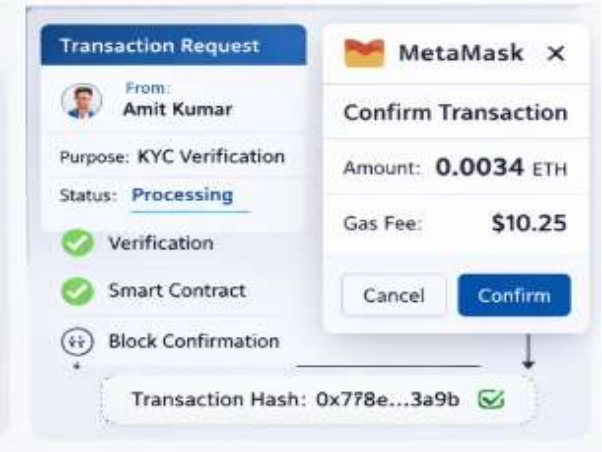

Fig 6.3: Smart Contract Execution

Fig 6.4: Decentralized Identity Execution

Fig 6.5: Score History

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
IJARST
ISSN: 2457-0362

Fig 6.6: System Statics

VII. CONCLUSION

This project presented a secure and transparent framework for Know Your Customer (KYC) management and credit scoring using blockchain technology. By replacing traditional centralized KYC systems with a decentralized blockchain-based approach, the framework eliminates redundant verification processes, reduces operational costs, and enhances data security. The use of cryptographic hashing and smart contracts ensures data integrity, privacy, and automation of verification and consent management. Additionally, integrating credit scoring within the same framework enables financial institutions to access reliable and tamper-proof credit assessments, improving trust and decision-making. Overall, the proposed system increases transparency, strengthens compliance, and provides users with greater control over their personal and financial data.

VIII. FUTURE SCOPE

In the future, this framework can be enhanced by integrating advanced machine learning models to generate more accurate and dynamic credit scores based on real-time financial behavior. The system can also be extended to support cross-border KYC interoperability, enabling global financial institutions to share verified identities securely. Incorporating decentralized identity (DID) standards and zero-knowledge proofs can further improve privacy by allowing identity verification without revealing sensitive data. Additionally, regulatory nodes can be introduced into the blockchain network to support real-time compliance monitoring. With the adoption of scalable blockchain platforms and integration with government digital identity systems, the framework has strong potential to become a unified digital identity and credit assessment solution for modern financial ecosystems.

IX. REFERENCES

[1]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2]. M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media, 2015. DOI: 10.1002/9781119334316

[3]. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016. DOI: 10.1109/ACCESS.2016.2566339

[4]. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 2000–2021, 2017. DOI: 10.1109/COMST.2017.2690444

[5]. G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in *Proc. IEEE Security and Privacy Workshops*, 2015, pp. 180–184. DOI: 10.1109/SPW.2015.27

[6]. M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A Global Naming and Storage System Secured by Blockchains," in *USENIX Annual Technical Conference*, 2016. DOI: 10.5555/3026877.3026923

[7]. A. M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, 2nd ed. Sebastopol, CA, USA: O'Reilly Media, 2017. DOI: 10.1007/978-1-4842-2604-9

[8]. H. Kim and M. Laskowski, "Toward an Ontology-Driven Blockchain Design for Supply Chain Provenance," *Intelligent Systems in Accounting, Finance and Management*, vol. 25, no. 1, pp. 18–27, 2018. DOI: 10.1002/isaf.1424

[9]. F. Casino, T. K. Dasaklis, and C. Patsakis, "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019. DOI: 10.1016/j.tele.2018.11.006

[10]. W. Wang, D. T. Hoang, X. Hu, et al., "A

[11]. Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019. DOI: 10.1109/ACCESS.2019.2896108

[12]. Y. Chen, S. Ding, Z. Xu, et al., "A Blockchain-Based Credit Evaluation System for Financial Services," *IEEE Access*, vol. 7, pp. 61021–61030, 2019. DOI: 10.1109/ACCESS.2019.2915001

[13]. M. Pilkington, "Blockchain Technology: Principles and Applications," in *Research Handbook on Digital Transformations*, 2016. DOI: 10.4337/9781784717766.00019

[14]. J. Xu, K. Xue, and P. Hong, "An IPFS-Based Storage Model for Blockchain," in *IEEE ICC Workshops*, 2018. DOI: 10.1109/ICCW.2018.8403650

[15]. E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *Proc. EuroSys*, 2018. DOI: 10.1145/3190508.3190538

[16]. S. Sharma, U. Ghosh, and A. Roy, "Blockchain-Based Secure Digital Identity Management Framework," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5539–5550, 2020. DOI: 10.1109/JSYST.2020.2993511