International Journal of Scientific Research in Engineering and Management (IJSREM)
Special Edition - Volume 09 NCFT -2025 SJIF Rating: 8.586 ISSN: 2582-3930

Enhanced Bank KYC Process using Ethereum Blockchain Framework

P Siddharth Krishna
Student, Computer Science and Engineering
Guru Nanak Institutions Technical Campus (Autonomous)
Hyderabad, Telangana, India-501506
krishnasiddharth91@gmail.com

Mohammed Mudassir Ahmed
Student, Computer Science and Engineering
Guru Nanak Institutions Technical Campus (Autonomous)
Hyderabad, Telangana, India-501506
mdahmeddvk@gmail.com

Mohammed Abdul Wasey
Student, Computer Science and Engineering
Guru Nanak Institutions Technical Campus (Autonomous)
Hyderabad, Telangana, India-501506
mdabdulwa3@gmail.com

Mrs. Hyma Birudaraju
Assistant Professor, Computer Science and Engineering
Guru Nanak Institutions Technical Campus (Autonomous)
Hyderabad, Telangana, India-501506
bhyma.gnitc@gniindia.org

***Abstract*—Ensuring compliance with regulatory requirements through efficient Know Your Customer (KYC) processes continues to pose a major challenge for financial institutions globally. Traditional KYC procedures are often inefficient, repetitive, and exposed to significant security risks such as identity fraud, data breaches, and inconsistent verification protocols. As consumer expectations for smooth digital banking interactions rise, current systems frequently fail to balance both security and operational efficiency. This paper introduces a blockchain-driven solution built on the Ethereum platform aimed at enhancing the security and effectiveness of KYC operations. By leveraging blockchain's decentralized structure, customer data is stored on a distributed ledger, which guarantees data integrity, transparency, and resistance to tampering. The proposed model also grants individuals greater control over their personal information, allowing them to selectively share data with financial institutions, thereby minimizing redundancy and strengthening privacy.**

Smart contracts are integrated into the system to automate the KYC verification steps, ensuring swift processing aligned with regulatory standards. Additionally, a central banking body is entrusted with managing a complete directory of all involved financial entities and monitoring their compliance with the rules enforced within the blockchain ecosystem.

I. INTRODUCTION

Financial institutions are increasingly required to verify customer identities with greater accuracy and speed. Know Your Customer (KYC) processes are essential in combating financial fraud and ensuring adherence to regulatory standards. However, conventional KYC approaches present numerous inefficiencies. Manual identity checks are not only time-consuming and expensive but also vulnerable to human error. Customers often have to submit the same documentation repeatedly to different organizations, which leads to frustration and delays.

A key challenge lies in protecting personal information. Traditional centralized databases that store sensitive data are attractive targets for cybercriminals. Data breaches can compromise individual privacy and lead to significant financial and reputational losses for organizations. As compliance regulations become more stringent, there is a growing need for smarter, more secure solutions to streamline KYC workflows. Blockchain technology offers a promising alternative. Its decentralized architecture removes reliance on a central authority for data validation. With built-in immutability and transparency, blockchain enables secure and efficient verification of customer information across multiple financial entities, while reducing data duplication. Ethereum, a leading blockchain platform, supports smart contracts — automated, self-enforcing agreements encoded directly into the blockchain. These smart contracts can handle critical parts of the KYC lifecycle, such as identity verification and user consent, with minimal human involvement, thereby increasing accuracy and efficiency.

This paper introduces a framework that utilizes Ethereum's capabilities to build a robust, privacy-preserving, and streamlined KYC system. In this model, users manage their own digital identities and grant selective access to financial institutions. Banks and related entities can validate customer data without redundant documentation requests, enhancing the user experience. A central authority monitors compliance to maintain system integrity and trust across the blockchain network.

II. RELATED WORK

The Know Your Customer (KYC) process has been a subject of continuous research due to its crucial role in regulatory compliance and fraud prevention. Traditional KYC systems, based on centralized storage and manual verification, have been criticized for inefficiency, vulnerability to cyberattacks, and duplication of effort across financial institutions. Researchers have explored multiple technological approaches to enhance KYC operations, including digital identity management systems,

biometric verification, and centralized data-sharing platforms.

Several studies have investigated the use of blockchain technology as a potential solution to the inefficiencies of conventional KYC frameworks. Zyskind et al. (2015) proposed a decentralized personal data management system using blockchain to give users control over their private information. Similarly, the concept of self-sovereign identity systems, as discussed by Tobin and Reed (2016), emphasizes user-centric control, where individuals manage their identity data without reliance on central authorities.

Specific to financial services, the Utility Settlement Coin project (2017) and initiatives like KYC-Chain have explored blockchain-based identity verification models for faster and more secure customer onboarding. These projects demonstrate that blockchain can streamline the KYC process by enabling institutions to share verified information, reducing duplication and operational costs.

Ethereum, with its capability to support programmable smart contracts, has further expanded blockchain's potential applications in KYC. Projects such as uPort and Sovrin have used Ethereum's decentralized architecture to develop platforms where users maintain and control access to their digital identities. These efforts have shown that blockchain can automate the validation and consent processes, minimizing manual interventions.

Despite these advancements, challenges remain. Many blockchain-based KYC solutions face issues related to interoperability, regulatory acceptance, data privacy laws (such as GDPR compliance), and scalability. Furthermore, few models adequately balance decentralization with necessary regulatory oversight, which is essential in financial sectors.

Our proposed work addresses these gaps by introducing a KYC framework that leverages Ethereum's smart contracts for verification automation while incorporating a centralized supervisory authority to monitor compliance. Unlike fully decentralized models, our approach ensures regulatory bodies maintain oversight, promoting trust among financial institutions and regulators. By combining decentralized identity management with centralized governance, the proposed system offers a practical pathway toward scalable, secure, and compliant KYC operations in the financial sector.

III. Problem Statement and Existing System

The current Know Your Customer (KYC) process used by financial institutions is highly fragmented, repetitive, and resource-intensive. Each bank or financial service provider collects and verifies customer identity documents independently, even if the same customer has already completed KYC elsewhere. This results in excessive duplication of efforts, increased onboarding time, and high operational costs for institutions. From a customer's perspective, the process is often frustrating, as they are required to submit similar documents repeatedly when interacting with different organizations.

In traditional KYC systems, customer data is stored in centralized databases managed individually by financial institutions. While this model provides direct control to organizations, it introduces significant vulnerabilities. Centralized repositories of sensitive data are common targets for cyberattacks, and a successful breach can expose thousands of personal records. Moreover, inconsistent data formats, outdated verification methods, and lack of interoperability across organizations make it difficult to build a standardized and reliable KYC framework.

Another key limitation of the existing system is the absence of real-time data sharing among institutions. When customer information changes, such as a new address or updated identification, the updates are often not reflected across all systems in a timely manner. This results in outdated or mismatched records, which can lead to compliance failures or rejected applications.

Additionally, the lack of a transparent audit trail makes it difficult for regulatory bodies to monitor KYC compliance across different institutions. Manual record-keeping and disjointed processes hinder effective oversight, exposing the system to risks of fraud, identity theft, and non-compliance penalties.

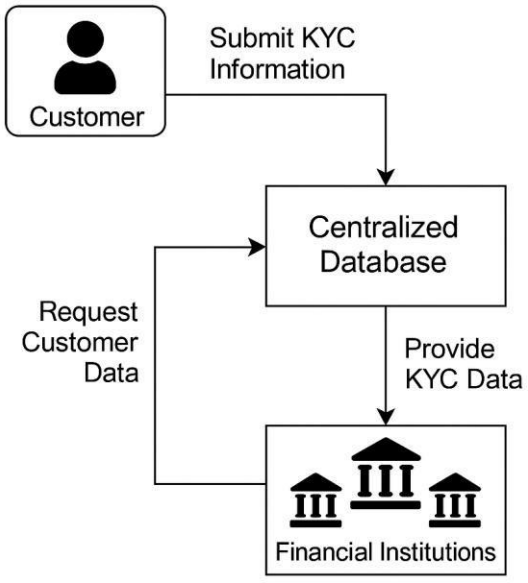

Fig: System Architecture of Existing System

From a technological standpoint, current KYC systems do not leverage modern tools for automation or secure data sharing. Processes such as document verification, address validation, and customer consent are still largely handled manually, leading to increased human error and inefficiencies. As digital transformation accelerates in the financial sector, these outdated systems struggle to keep pace with the demand for faster, more secure, and user-friendly services.

These challenges highlight the urgent need for an innovative KYC solution that reduces redundancy, enhances data privacy, promotes secure data sharing, and ensures real-time regulatory compliance. The shortcomings of the current system form the foundation upon which our proposed Ethereum blockchain-based KYC framework is built.

IV. Proposed System and Architecture

To overcome the limitations of traditional KYC systems, this paper proposes a decentralized framework built on the Ethereum blockchain. The core idea is to provide customers with a digital identity that they fully control, which can be securely shared with multiple financial institutions as needed. This eliminates repetitive document submissions and enables banks to access up-to-date, verified information instantly. Smart contracts on the Ethereum network are used to automate key verification and authorization processes, ensuring transparency, trust, and reduced human intervention.

In this system, every customer creates a digital KYC profile, which includes essential identity information such as name, address, ID proofs, and other regulatory details. This profile is hashed and stored on the Ethereum blockchain, while the actual documents are encrypted and saved off-chain in a secure distributed file system (e.g., IPFS). The blockchain only stores references (hashes) and access control records, ensuring both privacy and immutability.

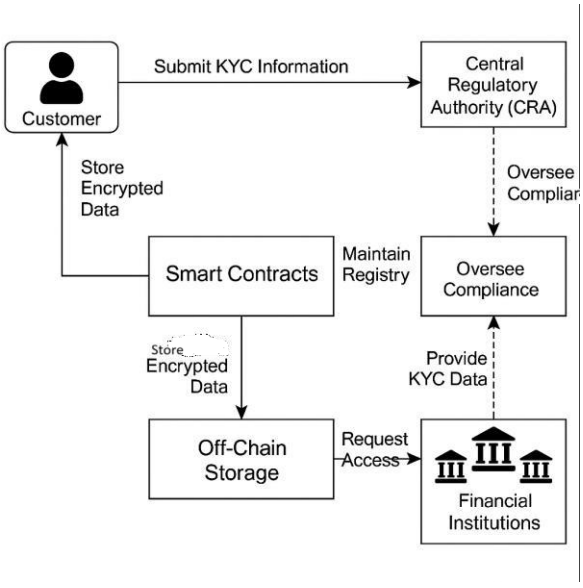

Fig: Smart Contracts for KYC System Architecture

Customers are given full control over their data. When they approach a financial institution for services, they can grant permission to access their verified KYC profile using blockchain-based access tokens. This permission is managed and enforced by smart contracts, which ensure that only authorized entities can view specific data. Once verified, the institution can use the data without repeating the full KYC process, saving time and cost.

A key component of this system is a **Central Regulatory Authority (CRA)**, such as a central bank, which oversees the entire blockchain network. The CRA maintains a registry of verified financial institutions, ensures that all smart contract rules comply with legal standards, and performs audit checks on data access events. While the system remains decentralized for identity management, the CRA ensures regulatory alignment and trust among participants.

1) *4.1 System Architecture Overview*

The architecture consists of the following components:

- **Customer Module**: Used to create, manage, and share personal identity data. Integrates wallet and user authentication.
- **Financial Institution Node**: Authorized entities that can request KYC data through smart contracts. Each institution runs a node that interacts with the Ethereum blockchain.
- **Ethereum Blockchain Layer**: Hosts the smart contracts, access tokens, audit trails, and hash links to off-chain data.
- **Off-chain Storage**: Encrypted storage of actual KYC documents. This layer ensures scalability and privacy.
- **Central Regulatory Authority (CRA)**: Monitors transactions, manages compliance, and maintains the permissioned registry of participants.

The flow of data and verification is secured using public-private key encryption. All access requests and updates are logged on the blockchain for transparency and traceability.

V. Algorithm Description

1) *Step-by-Step Workflow*

Step 1: User Onboarding and Profile Creation

- A customer initiates the KYC process via a secure user interface and submits personal identity information.
- The data is encrypted and stored on an external decentralized storage system (e.g., IPFS).
- A cryptographic hash of this data, along with metadata such as the timestamp, is recorded on the Ethereum blockchain to ensure integrity and traceability.
- The customer is assigned a unique blockchain address and corresponding key pair to manage permissions.

Step 2: Smart Contract Initialization

- A dedicated smart contract is deployed for each customer on the Ethereum network.

- This contract includes logic for permission management, data request handling, access control, and audit logging.
- The smart contract acts as the bridge between the user and authorized financial institutions.

Step 3: Financial Institution Enrollment

- Banks and other financial entities apply for participation via a Central Regulatory Authority (CRA).
- Upon approval, these institutions are issued blockchain credentials and listed in a verified registry contract, allowing them to interact with the KYC system.

Step 4: Request for KYC Access

- When an institution wants to access a customer's KYC profile, it sends a request to the customer's smart contract.
- The system notifies the user, prompting them to grant or deny access using a secure digital signature.

Step 5: Access Authorization and Data Retrieval

- Upon approval by the user, temporary access credentials are issued to the requesting institution.
- The institution retrieves the encrypted data from the external storage and decrypts it using a shared key.
- All interactions — including consent, access, and data handling — are permanently logged on the blockchain.

Step 6: Regulatory Oversight and Auditing

- The CRA routinely audits smart contract logs to ensure compliance with regulatory guidelines.
- Each event on the blockchain is immutable, timestamped, and available for traceability, ensuring accountability across the ecosystem.

2) Key Highlights of the Algorithm

- **Decentralized Identity Ownership:** Customers maintain full control over their identity data.
- **Automated Compliance:** Smart contracts enforce regulatory requirements without human intervention.
- **Interoperability:** Once verified, customer identity is reusable across multiple institutions, eliminating repetitive checks.
- **Transparent Auditing:** Every action in the system is traceable and cannot be altered, facilitating compliance monitoring.

VI. Advantages and Limitations

A. Advantages of the Proposed System

1. Enhanced Security and Data Privacy

Leveraging blockchain technology provides a tamper-proof, cryptographically secure environment for storing customer data. Since the information is encrypted and only accessible with the user's explicit consent, the risks of unauthorized access and data breaches are significantly minimized.

2. User-Centric Identity Control

Unlike conventional systems where financial institutions own and manage customer information, this framework gives users full autonomy over their digital identities. They can selectively grant, limit, or revoke data access at any time, aligning with privacy-focused standards.

3. Reduced Redundancy and Operational Costs

Once a customer's identity has been verified through the system, it can be reused by other participating institutions without repeating the KYC process. This reduces repetitive documentation efforts, shortens onboarding durations, and lowers administrative expenses for financial firms.

4. Real-Time Transparency and Auditability

Every transaction — including data requests, access logs, and updates — is immutably recorded on the Ethereum blockchain. This enables continuous monitoring and auditing by regulatory bodies, ensuring transparency and accountability within the network.

5. Smart Contract-Driven Automation

Key aspects of KYC verification, such as consent management and access control, are automated using smart contracts. This reduces dependency on manual intervention, improves efficiency, and ensures adherence to regulatory rules with minimal error.

6. Balanced Regulatory Supervision

The integration of a Central Regulatory Authority (CRA) provides oversight while maintaining the decentralized nature of the system. The CRA manages a verified list of financial institutions and monitors system activity, fostering trust among participants through a hybrid governance model.

B. Limitations of the System

1. Scalability Constraints

Ethereum's current infrastructure poses challenges in terms of transaction speed and cost-efficiency. High gas fees and limited throughput can hinder widespread KYC adoption without adopting Layer 2 scaling solutions or alternative platforms.

2. Off-Chain Data Storage Challenges

Due to storage and privacy limitations, sensitive documents cannot be kept directly on the blockchain. The reliance on external storage solutions (such as IPFS) introduces complexities in data integrity, synchronization, and security management.

3. Legal and Regulatory Ambiguities

Despite the technological readiness, many jurisdictions lack comprehensive legal frameworks to support blockchain-based identity systems. Aligning the framework with evolving global privacy regulations — such as GDPR and India's DPDP Act — remains an ongoing concern.

4. Institutional Resistance and Integration Complexity

Traditional financial organizations may resist adopting blockchain due to legacy infrastructure, operational inertia, or skepticism about the technology's maturity. Overcoming these barriers requires strong stakeholder engagement and robust integration strategies.

VII. Results and Discussion

Although the proposed Ethereum-based KYC framework is currently conceptual and has not yet been deployed at scale, the expected outcomes can be analyzed based on a comparison of its functional design with conventional KYC systems. Through theoretical modeling and analysis of existing blockchain use cases in financial applications, several measurable benefits emerge from this approach.

7.1 Expected Performance Improvements

By removing redundant data collection and leveraging smart contracts for identity validation, the system is projected to reduce customer onboarding time significantly. In traditional systems, KYC verification can take several days to complete due to manual checks and document verification. With blockchain-enabled automation and data reuse, this process could be shortened to a few minutes, especially for returning users whose identities are already validated on the network.

Additionally, operational costs associated with identity verification are expected to decrease. Studies have shown that financial institutions spend billions globally on KYC compliance annually. By automating the majority of these tasks and eliminating repeated efforts across institutions, the proposed system could result in cost savings of up to 40–60% over time.

7.2 Improved User Experience

One of the major qualitative results anticipated from this system is an enhanced customer experience. Users will no longer need to resubmit the same identity documents to multiple banks, nor wait extended periods for verification. Instead, they will have control over their data and can authorize secure sharing in real-time, making the experience more convenient, private, and empowering.

7.3 Security and Transparency

The use of public-key encryption and blockchain immutability enhances data security. Because all access events are logged transparently, customers and regulators alike can track when, where, and by whom data is accessed. This addresses concerns of unauthorized use and builds trust in the system. Compared to traditional centralized databases, the distributed nature of Ethereum nodes reduces the risk of single points of failure or targeted breaches.

7.4 Regulatory Use Case

A notable result of integrating a Central Regulatory Authority (CRA) is the ability to maintain compliance across a decentralized environment. The CRA can perform audits by reviewing blockchain logs, ensuring that no unauthorized access occurred, and that all data usage complies with regulatory standards. This hybrid model (user-owned data with centralized oversight) combines the strengths of decentralization with real-world compliance needs.

7.5 Limitations of Evaluation

While the design appears robust in theory, real-world performance will depend on network congestion, gas fees, and interoperability with off-chain storage systems. The next phase of this project will involve simulating the framework using test environments like Ethereum's Rinkeby or Sepolia testnets, along with tools such as Ganache and Truffle Suite to measure transaction times and smart contract execution behavior.

In summary, the proposed blockchain-based KYC system offers promising results in terms of efficiency, cost reduction, data privacy, and compliance transparency. Real-world deployment and performance testing will further validate these findings.

VIII. Conclusion and Future Work

This paper presents a blockchain-based framework using the Ethereum platform to improve the Know Your Customer (KYC) process in the banking sector. Traditional KYC methods are time-consuming, costly, and prone to data duplication and security risks. The proposed system addresses these issues by decentralizing identity management, automating verification through smart contracts, and allowing customers to control their data.

By integrating a Central Regulatory Authority, the framework maintains compliance and transparency, ensuring that access to customer data is properly monitored and logged. The system offers improved data security, faster onboarding, reduced costs, and enhanced user privacy.

While the design offers promising improvements, challenges such as scalability, legal compliance, and integration with existing systems remain. Future work will involve developing a working prototype, testing it in simulated environments, and exploring features like biometric integration and cross-chain interoperability.

Overall, the proposed model lays a foundation for a secure, efficient, and compliant digital identity verification system, aligned with modern banking needs and technological advancements.

REFERENCES

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

[2] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," *Ethereum White Paper*, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/

[3] M. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Priv. Workshops*, pp. 180–184, May 2015.

[4] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *Sovrin Foundation*, June 2016. [Online]. Available: https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

[5] C. Allen, "The path to self-sovereign identity," *Life With Alacrity Blog*, Apr. 2016. [Online]. Available: https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

[6] KYC-Chain, "KYC-Chain: Blockchain-based KYC solutions," [Online]. Available: https://www.kyc-chain.com/

[7] S. Chen, X. Shi, Y. Ren, and H. Yan, "A blockchain-based KYC framework using smart contracts," *Int. J. Network Security*, vol. 22, no. 1, pp. 59–68, Jan. 2020.

[8] A. Deshpande, K. Stewart, L. Lepetit, and V. Gunashekar, "Distributed ledger technologies/blockchain: Challenges, opportunities and the prospects for standards," *British Standards Institution (BSI)*, 2017.

[9] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World*, Penguin, 2016.

[10] J. Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*, Wiley, 2016.

[11] S. B. P. Kumar and R. Chatterjee, "Secure KYC for banking using blockchain technology," in *Proc. Int. Conf. Emerg. Technol. Trends Electron., Commun. and Networking*, pp. 1–6, Dec. 2018.

[12] R. T. Goyal and K. Jain, "Blockchain-based identity management systems: A review," *Int. J. Computer Applications*, vol. 182, no. 39, pp. 25–30, 2019.

[13] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," *Extropy*, vol. 16, 1996. [Online].

Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

[14] J. Klinger, J. McMullen, and C. S. Dinesh, "Digital identity: An analysis of the literature," *MIT Digital Currency Initiative*, 2020. [Online]. Available: https://dci.mit.edu/research

[15] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*, F. Xavier Olleros and M. Zhegu, Eds. Edward Elgar Publishing, 2016, pp. 225–253.

[16] https://www.socure.com/glossary/identity-verification

[17] Blockchain for Secure Data Management: Ensuring Integrity and Transparency
By Ronald Mccarthy
https://www.developernation.net/blog/blockchain-for-secure-data-management-ensuring-integrity-and-transparency/

[18] Cost Per Digital Identity Verification Checks to Drop 15% Globally by Thomas Wilson
https://www.juniperresearch.com/resources/infographics/cost-per-digital-identity-verification-checks-to-drop-15-globally