WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Decentralized KYC: Empowering Banks with Ethereum Blockchain

Megha Dabas[1], Thakur Mohit Singh[2], G. Sai Gautham[3], Pradeepthi Kaniki[4], Sameeksha Reddy[5]

[1]Assistant Professor, Computer Science and Engineering, Guru Nanak Institutions Technical Campus Telangana, India
meghaharshudabas@gmail.com
[2,3,4,5]Computer science and Engineering (internet of things) Guru Nanak Institutions Technical Campus Telangana, India
[2]mohitthakursingh@gmail.com, [3]saigoutham144@gmail.com, [4]pradeepthikanikireddy@gmail.com, [5]Sameekshareddy456@gmail.com

ABSTRACT –

The Know Your consumer (KYC) process, which ensures the security and legality of consumer identity, is a requirement for financial institutions to comply with regulatory standards. With its immutability, security, and transparency, blockchain technology presents a ground-breaking approach to enhancing the KYC process. By using decentralized platforms like Ethereum, blockchain technology enables more efficient and cost-effective customer data management. This significantly reduces the amount of time and money required for compliance. Blockchain technology can help banks overcome the challenges they have when conducting KYC and customer onboarding. To ensure that large payments are accurately recorded and authenticated, it also puts in place a system that demands KYC identity for clients who make significant transactions that exceed a predefined threshold. A central regulatory body oversees the thorough registration of financial firms and rigorously enforces KYC regulations in the proposed architecture. In addition to improving security, reducing fraud, and ensuring compliance, this solution provides a quick and efficient process for safely handling both routine and complex transactions.

Keywords - Blockchain, Ethereum, Smart Contracts, KYC, Decentralization, Data Privacy, Customer Onboarding, AML, Transparency

I. Introduction

In the constantly changing financial world of today, banks under tremendous pressure to swiftly enroll new clients while adhering to stringent regulatory requirements. Know Your Customer (KYC) is a series of steps intended to confirm the identification of customers and evaluate the risk they represent. It is one of the most important and time-consuming steps in this process. KYC has historically been administered centrally, with each institution gathering, keeping, and validating client information on its own. This creates needless effort duplication and presents issues with cost, inefficiency, and data privacy.

Blockchain technology is becoming a potent instrument to tackle these issues, especially decentralized platforms like Ethereum. Blockchain's fundamental ideas of distributed consensus, transparency, and immutability have the potential to completely transform KYC procedures. By removing the need for repeated verifications and preserving strict control over data access and integrity, a decentralized KYC system enables banks and other financial institutions to securely exchange confirmed client data.

By making the onboarding process quicker, safer, and more affordable, a blockchain-based decentralized KYC system that uses Ethereum can empower banks. It describes the architecture of a decentralized solution, points out the drawbacks of the existing KYC techniques, and looks at how Ethereum smart contracts may automate trust without the need for centralized authority. In the end, this strategy seeks to create a more cohesive and effective financial ecosystem by striking a balance between client convenience and regulatory compliance.

In the digital era, banking systems are always changing to satisfy the needs of a clientele that is expanding quickly and becoming more tech-savvy. The Know Your Customer (KYC) procedure is one of the most important parts of any financial institution's operations. In order to avoid money laundering, terrorism funding, identity theft, and other types of financial fraud, KYC entails confirming clients' identities prior to offering them financial services.

The traditional KYC procedure is still quite centralized and duplicated despite its significance. Even if another bank has already finished the procedure, each financial institution must individually gather, validate, and store client data. In addition to causing redundant work and higher operating expenses, this also creates inefficiencies that may cause client onboarding to lag. Centralized storage systems are also susceptible to data tampering and breaches, which raise serious questions regarding the security and privacy of private client data.

The promise of blockchain technology to safeguard and decentralize digital processes across sectors has drawn attention from all around the world in recent years. One of the most well-known blockchain systems, Ethereum, provides a decentralized, programmable framework that may allow smart contracts for safe, transparent, and unchangeable applications. Because of these characteristics, it's a great option to reconsider how banking institutions handle KYC procedures.

Once a customer's identification has been confirmed by a reliable bank or agency, blockchain technology may be used to safely exchange that information with other approved organizations. Only authorized and validated entities may access this data thanks to smart contracts, and any adjustments or verifications are permanently noted on the ledger.

This method greatly lowers operating expenses, data silos, and compliance obligations while simultaneously improving transparency and auditability. Additionally, because they may grant and withdraw access to institutions as required, it gives customers more control over their personal data. In a tamper-proof environment, the decentralization of KYC also promotes improved cooperation between banks, fintech firms, regulators, and identity suppliers.

II. Literature Review

The Know Your Customer (KYC) process is a cornerstone of modern banking compliance, designed to prevent fraud and maintain regulatory standards. Over the years, numerous studies and innovations have aimed to improve the KYC process, particularly in terms of cost-efficiency, data privacy, and interoperability. However, the conventional centralized KYC systems have remained plagued by redundancies, fragmented data handling, and rising operational burdens. This literature review explores the body of work surrounding KYC challenges and how blockchain—especially Ethereum—is emerging as a transformative solution.

I. Traditional KYC Systems

Scholars and industry experts have long highlighted the inefficiencies in traditional KYC procedures. According to the Financial Conduct Authority (FCA) and World Bank reports, banks can spend millions annually on repeated KYC efforts, especially when onboarding corporate clients. Each institution collects and verifies the same data independently, causing delays and inconsistencies. Fatima et al. (2020) emphasize the risks of data breaches in centralized systems, citing a lack of transparency, limited customer control, and susceptibility to cyberattacks. Their research suggests that centralization not only increases costs but also puts customer data at greater risk due to single points of failure.

II. Blockchain in KYC

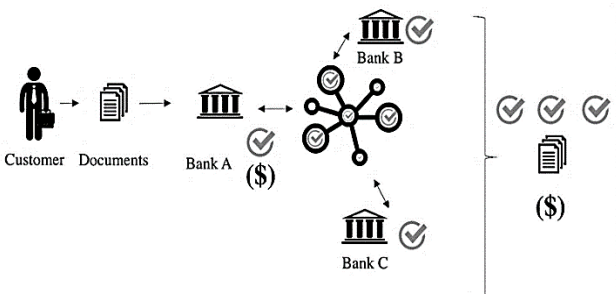
Blockchain technology has drawn significant attention for its potential to transform identity verification. Zyskind et al. (2015) proposed a decentralized framework for data ownership and access control, using blockchain to give users more control over their personal information. Meijer and van der Veer (2019) reviewed the application of blockchain in KYC and concluded that distributed ledgers could provide a single source of verified truth shared across multiple banks. This eliminates redundant checks and creates auditability while reducing compliance costs. Their findings emphasize that blockchain can support trust without central authorities through cryptographic mechanisms and consensus algorithms.

III. Ethereum's Role and Practical Implementations

Ethereum has become a popular choice for building decentralized KYC systems due to its smart contract capabilities. Research by Christidis and Devetsikiotis (2016) highlighted Ethereum's strength in automating access control and trust management using programmable logic. Moreover, identity platforms like uPort, Civic, and SelfKey (built on or compatible with Ethereum) demonstrate the feasibility of self-sovereign identity systems in real-world banking use cases. Patel and Shah (2022) showed how Ethereum-based smart contracts can enable efficient multi-party verification, where KYC data verified once can be reused securely across multiple institutions. Their work further underlines Ethereum's capability to enforce dynamic data-sharing policies without compromising user privacy.

IV. Regulatory Considerations and Limitations

Despite its promise, blockchain-based KYC must address critical legal and regulatory challenges. Mavroeidi et al. (2020) caution against storing personally identifiable information directly on public blockchains, which may violate data protection laws like GDPR. Instead, they propose hybrid models that use off-chain storage linked with on-chain verification hashes. Further, regulatory acceptance of decentralized systems remains varied across jurisdictions. While countries like Estonia and Singapore encourage blockchain innovation, others still rely on rigid compliance structures, slowing down adoption..



III. Methodology

This study uses a mixed-method approach to assess the viability and benefits of a decentralized KYC system utilizing Ethereum, including both technical prototype implementation and qualitative examination of current systems.

Using the Ethereum blockchain and its smart contract features, a decentralized KYC architecture was created. To handle permissioned access to KYC data, track user consent, and manage identity approvals, the system makes use of Ethereum smart contracts. In order to prevent the direct storage of sensitive data on the blockchain, the architecture incorporates IPFS, an off-chain storage system that securely stores documents and allows access through on-chain hash references.

In order to ascertain the usefulness of the suggested model, a comparison between traditional and decentralized KYC procedures was carried out. Onboarding time, compliance overhead, security levels, and user happiness were among the criteria. Legal counsel and industry experts' opinions were included to guarantee practical applicability. According to the feedback, a decentralized method gives users more control over their information, improves audit trails, and eliminates redundancy.

A. System Analysis and Requirement Gathering

To start, a thorough examination of conventional KYC procedures in banking was carried out using case studies and a review of the literature. This made it easier to pinpoint major issues such data duplication, expensive verification, and delays in compliance. Decentralized identity verification, smart contract-based access management, and user-centric data ownership were among the elements that were deemed necessary for the proposed blockchain-based KYC system.

First, using case studies and a review of the literature, a thorough examination of conventional KYC procedures in banking was carried out. This made it easier to pinpoint major issues such data duplication, expensive verification, and delays in compliance. After that, specifications for the suggested blockchain-based KYC system were established, encompassing attributes such as user-centric data ownership, smart contract-based access management, and decentralized identity verification.

B. Blockchain Architecture Design

Using smart contracts, an Ethereum-based architecture was created to store and handle KYC permits and approvals. The architecture makes use of hash values and IPFS (InterPlanetary File System) for off-chain document storage in place of directly storing sensitive material on-chain. Workflows for interbank verification, regulator access, and user consent are managed by the smart contract. The contract functionality was implemented and simulated using programs like Solidity, Truffle Suite, and MetaMask.

C. Simulation and Functional Testing

To replicate inter-bank KYC sharing scenarios, the suggested solution was implemented on the Rinkeby test network for Ethereum. Cross-bank data retrieval, authorization granting and revocation, and client onboarding were among the test cases. The efficiency of the system was assessed by measuring key performance characteristics such transaction speed, cost (gas usage), and data integrity validation.

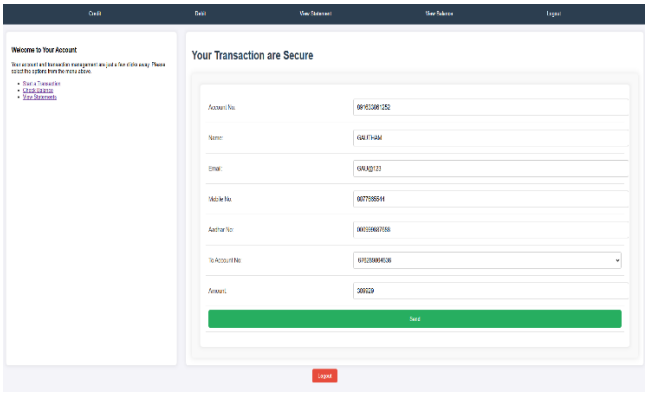
D. Comparative Evaluation

A study was carried out to compare the suggested decentralized method with the conventional KYC strategy. Data security, compliance expenses, onboarding duration, and auditability were among the criteria. In order to confirm the design's viability, input from white papers and industry specialists was also taken into account.

This methodology shows the practicality of integrating Ethereum blockchain into banking KYC procedures and enables a comprehensive knowledge of the efficacy of the suggested system.

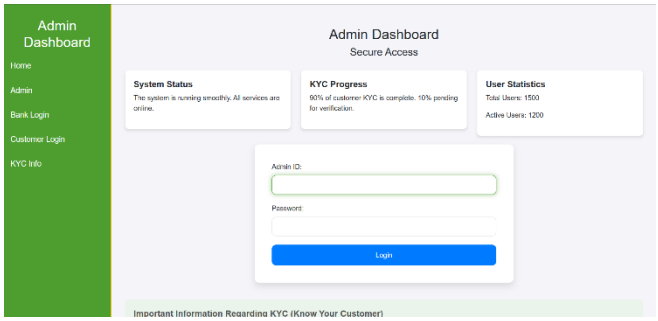
Lastly, a legal viability study was carried out in conjunction with data security experts. Examining the system's adherence to the GDPR, the Personal Data Protection Bill of India, and other global data privacy regulations was part of this. Due to legal issues with directly storing identifying data on public blockchains, the system makes sure that all personal information stays off-chain, with blockchain being utilized only for permission management and hashed pointer storage. In addition to adhering to privacy laws, this strategy facilitates cross-border compliance, which allows the model to be modified to fit different regulatory contexts.

Overall, this technique guarantees a comprehensive investigation of the operational, legal, and technical aspects of deploying Ethereum-based decentralized KYC. By discussing the advantages and disadvantages of the suggested system, the study provides a comprehensive viewpoint on the viability of blockchain-driven change in the banking industry.



An evaluation of the current KYC systems in financial institutions was the main objective of the first phase. The issues with redundancy and manual verification, data protection, documentation requirements, and current operational workflows were all reviewed. The analysis's conclusions influenced the development of the system requirements for a decentralized substitute, with a focus on data protection regulations, transparency, interoperability, and cryptographic security.

Later, an Ethereum blockchain-based smart contract-based architecture was created. The solution encodes smart contracts that control access permissions, user consent procedures, and identity verification procedures using Solidity. In order to maintain privacy standards, personal information is not kept on the blockchain itself. Rather, confidential papers are off-chain and encrypted using the InterPlanetary File System (IPFS).



IV. Implementation

The development of a safe, open, and automated identity verification system that lets consumers keep control over their personal information while granting financial institutions access to validated records with consent is the goal of implementing a decentralized KYC system using the Ethereum blockchain. This method takes the place of conventional centralized KYC methods, which are frequently prone to delays, redundancies, and inconsistent verification processes.

A blockchain-based infrastructure is used to store and preserve each user's digital identity, which is the foundation of the system. Consumers sign up for the network by providing their identification documents and personal information to a reliable organization, which then confirms and authenticates the data.

After a successful validation, a smart contract creates and records a hashed reference to the data on the Ethereum blockchain. The real papers are kept off-chain in encrypted form using safe storage platforms like the Interplanetary File System (IPFS). This division keeps private information off of a public ledger and guarantees adherence to privacy laws With the Truffle development environment, the implementation was run and tested on Ethereum's Rinkeby test network. To assess important use cases, including cross-institutional verification, access revocation, client onboarding, and audit trails initiated by smart contracts, a number of functional scenarios were simulated. Smart contract behavior, transaction speed, and gas efficiency were examined to make sure the system operates dependably in practical settings.

This level of cross-platform interoperability opens doors for secure and transparent educational data exchange between different institutions. For example, a certificate written to a student’s blockchain contract via a Moodle-based LMS could be accessed and verified by another institution running an edX-based platform—without compromising data ownership or privacy.

In addition, the prototype was constructed using a web front-end and a user-centric interface to illustrate how banks and customers interact. Customers were able to examine and approve or reject data access requests in real time using the interface, which gave the procedure an extra degree of control and transparency.

This application shows how the Ethereum blockchain can greatly lower the risks and overhead related to KYC procedures while enhancing user experience, data integrity, and institutional confidence when combined with smart contracts and off-chain encrypted data storage.

V. Conclusion

This study demonstrates how the Ethereum blockchain can streamline and improve the banking industry's KYC procedure. Financial organizations may speed onboarding, improve data security, and cut down on redundancy by switching to a decentralized approach. Off-chain storage guarantees adherence to data protection regulations, and smart contracts automate identity verification while granting users control over their data. Although there are still legal and technical obstacles to overcome, the suggested framework offers a workable, safe, and expandable solution. To facilitate the wider deployment of decentralized KYC systems, future initiatives should concentrate on standardization and regulatory integration.

The study validates that implementing decentralized KYC on Ethereum is technically feasible by designing and testing a prototype system. By empowering consumers to take control of their identity data and granting banks permission to access verified information, the system lowers operating expenses and onboarding time. Better adherence to legal and regulatory requirements is also ensured by the audit trails built into blockchain technology. There are still obstacles in the way of broad adoption, particularly with regard to institutional interoperability and jurisdiction-specific differences in regulatory preparedness. Future research should concentrate on developing collaborative governance models and standardized frameworks that facilitate legal compliance, user trust, and interoperability at scale.

Modern, safe, and effective identity verification systems must replace antiquated, centralized ones as banking practices change. This study has shown that by improving data security, raising transparency, and minimizing effort duplication among financial institutions, Ethereum-based decentralized KYC frameworks provide notable advantages over conventional approaches. Off-chain encrypted storage guarantees user privacy and regulatory compliance, while smart contracts allow automated, tamper-proof verification process execution.

For the financial industry, including Ethereum blockchain technology into the KYC procedure is a revolutionary move. It opens the door for a user-centered, decentralized ecosystem that improves operational effectiveness while fortifying security and trust in online financial transactions.

VI. REFERENCES

[1] H. Alanzi and M. Alkhatib, ‘‘Towards improving privacy and security of identity management systems using blockchain technology: A systematic review,’’ Appl. Sci., vol. 12, no. 23, p. 12415, Dec. 2022.

[2] Y. Chen, Y. Lu, L. Bulysheva, and M. Y. Kataev, ‘‘Applications of blockchain in Industry 4.0: A review,’’ Inf. Syst. Frontiers, vol. 24, pp. 1–15, Feb. 2022.

[3] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, ‘‘A survey on blockchain technology: Evolution, architecture and security,’’ IEEE Access, vol. 9, pp. 61048–61073, 2021.

[4] J. Dorminey, A. S. Fleming, M.-J. Kranacher, and R. A. Riley, ‘‘The evolution of fraud theory,’’ Issues Accounting Educ., vol. 27, no. 2, pp. 555–579, May 2012.

[5] F. C. Hui, V. C. Koneru, N. M. Ali, and S. Harun, ‘‘Implementing peer group analysis within a track and trace system to detect potential frauds,’’ Int. J. Supply Chain Manage., vol. 3, pp. 52–56, Jan. 2014.

[6] R. Patel, M. Migliavacca, and M. E. Oriani, ‘‘Blockchain in banking and finance: A bibliometric review,’’ Res. Int. Bus. Finance, vol. 62, Dec. 2022, Art. no. 101718.

[7] Q. Gan, R. Y. K. Lau, and J. Hong, ‘‘A critical review of blockchain applications to banking and finance: A qualitative thematic analysis approach,’’ Technol. Anal. Strategic Manage., vol. 33, pp. 1–17, Sep. 2021.

[8] J. Gomes, S. Khan, and D. Svetinovic, ‘‘Fortifying the blockchain: A systematic review and classification of post-quantum consensus solutions for enhanced security and resilience,’’ IEEE Access, vol. 11, pp. 74088–74100, 2023.

[9] M. A. Hannan, M. A. Shahriar, M. S. Ferdous, M. J. M. Chowdhury, and M. S. Rahman, ‘‘A systematic literature review of blockchain-based e-KYC systems,’’ Computing, vol. 105, no. 10, pp. 2089–2118, Oct. 2023.

[10] P. K. Ozili, ‘‘Decentralized finance research and developments around the world,’’ J. Banking Financial Technol., vol. 6, no. 2, pp. 117–133, Oct. 2022.

[11] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, ‘‘A survey on blockchain for information systems management and security,’’ Inf. Process. Manage., vol. 58, no. 1, Jan. 2021, Art. no. 102397. [12] S. Haber and W. S. Stornetta, ‘‘How to time-stamp a digital document,’’ J. Cryptol., vol. 3, no. 2, pp. 99–111, Jan. 1991.

[13] V. Kumar C and P. Selvaprabhu, ‘‘An examination of distributed and decentralized systems for trustworthy control of supply chains,’’ IEEE Access, vol. 11, pp. 137025–137052, 2023.

[14] S. Nakamoto, ‘‘Bitcoin: A peer-to-peer electronic cash system,’’ Decentralized Bus. Rev., vol. 4, no. 2, p. 15, Jan. 2008.

[15] M. M. Islam, Md. K. Islam, M. Shahjalal, M. Z. Chowdhury, and Y. M. Jang, ‘‘A low-cost cross-border payment system based on auditable cryptocurrency with consortium blockchain: Joint digital currency,’’ IEEE Trans. Services Comput., vol. 16, no. 3, pp. 1616–1629, May 2022.

[16] N. Kapsoulis, A. Psychas, G. Palaiokrassas, A. Marinakis, A. Litke, and T. Varvarigou, ‘‘Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture,’’ Future Internet, vol. 12, no. 2, p. 41, Feb. 2020.