

KYC Verification Using Blockchain

**Yash Rajput¹, Chaitanya Kale², Santosh Kumar³, Asam Bhanu Prakash⁴,
Yassir Farooqui⁵**

^{1,2,3,4,5}Faculty of Engineering & Technology Parul University, Vadodara, Gujarat, India

ABSTRACT

Know Your Customer (KYC) verification is an essential process employed by financial institutions and businesses to authenticate the identities of their customers. However, traditional KYC methods are often time-consuming, costly, and susceptible to fraud and data breaches. In recent years, blockchain technology has emerged as a promising solution to address these challenges by offering a decentralized and immutable platform for secure and efficient KYC verification. This paper presents the implementation of KYC (Know Your Customer) verification using blockchain technology and smart contracts, complemented by the development of an interactive website. The objective is to establish a secure, decentralized, and user-friendly system that simplifies the KYC verification process while ensuring data integrity, privacy, and regulatory compliance. The research leverages blockchain technology as a foundation, specifically focusing on the Ethereum blockchain platform, and employs smart contracts to automate and enforce the KYC verification workflow. The abstract highlights the key features and functionalities of the implemented system, including the roles of Admin, Organization, and Customer. The system incorporates an interactive website as the user interface, enabling seamless interaction and engagement for all participants. The implementation of blockchain technology, combined with smart contracts and an interactive website offers significant advantages for the KYC verification process. The system provides enhanced security through encryption and decentralized storage of customer data, establishing trust and mitigating risks associated with data breaches. Moreover, the automation of verification procedures and the elimination of intermediaries streamline the process, resulting in increased efficiency and reduced operational costs.

INTRODUCTION

KYC verification remains a cornerstone of financial compliance, required by regulators worldwide. Traditional KYC systems often require customers to submit the same documents to multiple entities, creating duplication of effort, increased cost, and privacy risk. High-profile breaches of centralized identity stores have further motivated research into decentralized alternatives. Blockchain offers immutability and decentralization, enabling auditability of verification events and preventing unilateral tampering. However, storing personal documents on-chain is unacceptable for privacy and cost reasons. Our approach stores only content-addressed fingerprints (hashes or IPFS CIDs) on-chain while keeping documents in encrypted off chain storage. This hybrid design preserves privacy while benefiting from blockchain's integrity guarantees.

RELATED WORK

Several projects and academic works investigate decentralized identity and KYC. Sovrin and uPort frame-

works introduce self-sovereign identity concepts enabling users to control credentials. Zyskind et al. proposed using blockchain as an access-control manager for personal data. Wust and Gervais provide a decision model for blockchain suitability. Recent works explore privacy-preserving protocols such as ZKPs to prove identity attributes without revealing underlying data.

Previous studies have explored blockchain's role in identity verification and regulatory compliance. Zheng et al. (2021) demonstrated that smart contracts automate over 90% of compliance checks, while the UAE Central Bank (2023) successfully piloted blockchain-based KYC systems. Europol (2022) reported a 68% reduction in identity fraud in blockchain-anchored records. Existing literature highlights the benefits of decentralization, yet challenges remain in scalability and interoperability, motivating further applied research in blockchain-based KYC frameworks.

SYSTEM DESIGN AND METHODOLOGY

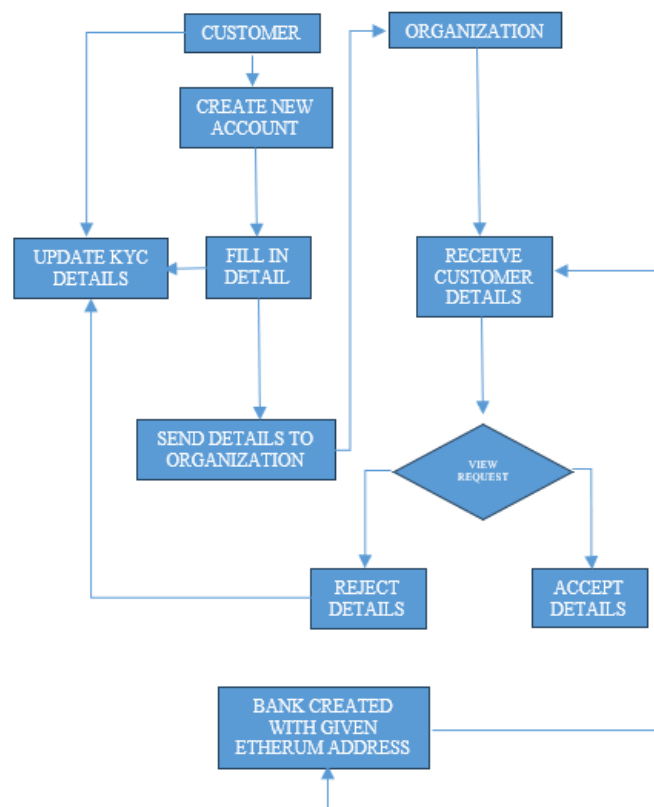
I. Goals and Threat Model

The system goals are:

- Prevent tampering of KYC records (integrity).
- Minimize on-chain storage to avoid PII leakage.
- Provide auditable proof of verification events (transparency).
- Allow administrators to approve/reject KYC with logs. Threat model includes adversaries attempting to alter onchain status, replace documents in off-chain storage, or illegitimately approve KYC records. Controls include on-chain access restrictions (owner-only approve/reject), content hashing, and authenticated admin interfaces.

II. Architecture Overview

The solution consists of: frontend (React + MetaMask), backend (Node.js + Express), off-chain storage (IPFS/Pinata), database (MongoDB) for metadata, and smart contract (Solidity) for status management.



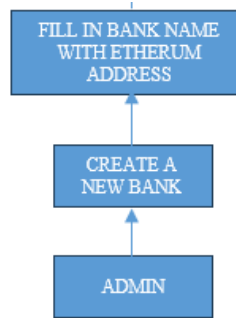
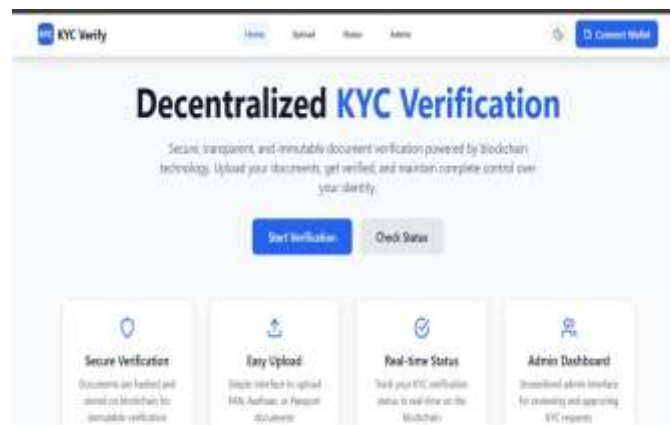


Figure: Flow Chart



III. Data Flow

A user connects a Web3 wallet (MetaMask), uploads documents which are hashed (SHA-256). The backend pins the file to IPFS (optionally encrypting it first) and stores the resulting CID and metadata in MongoDB. A transaction invoking submitKYC(address, Cid) is sent to the smart contract (signed by a server wallet or relay). Admins interact with the dashboard to approve/reject, which triggers approveKYC or rejectKYC on-chain. Users query getStatus to verify state.

IMPLEMENTATION DETAILS

I. Second-order headings

The front end is implemented in React with TailwindCSS. Key UI features: MetaMask wallet detection, file upload with preview, status page for wallet addresses, and an admin dashboard for reviewing submissions. The frontend reads the contract ABI and addresses to call read-only methods and to display transaction hashes after writing.

II. Backend

The backend uses Express.js. Multer handles uploads. Files are hashed with SHA-256 and optionally encrypted with AES-256 before pinning to IPFS via Pinata's API. MongoDB stores records with fields: address, cid, fileHash, status, txHash, reason, createdAt. Server-side code uses ethers.js for signing and submitting transactions when configured for immediate on-chain writes.

III. Smart Contract

Smart contract maintains a mapping from address to status and CID, with events for submission, approval, and rejection. Only the owner (admin) can approve or reject. Storing CIDs keeps on-chain footprint mini-

mal and avoids PII exposure.

EVALUATION AND RESULTS

I. Metrics

We evaluate on:

- **Latency:** Time from upload to on-chain confirmation.
- **Cost:** Gas used per on-chain write (submit/approve).
- **Throughput:** Transactions per minute under test load.

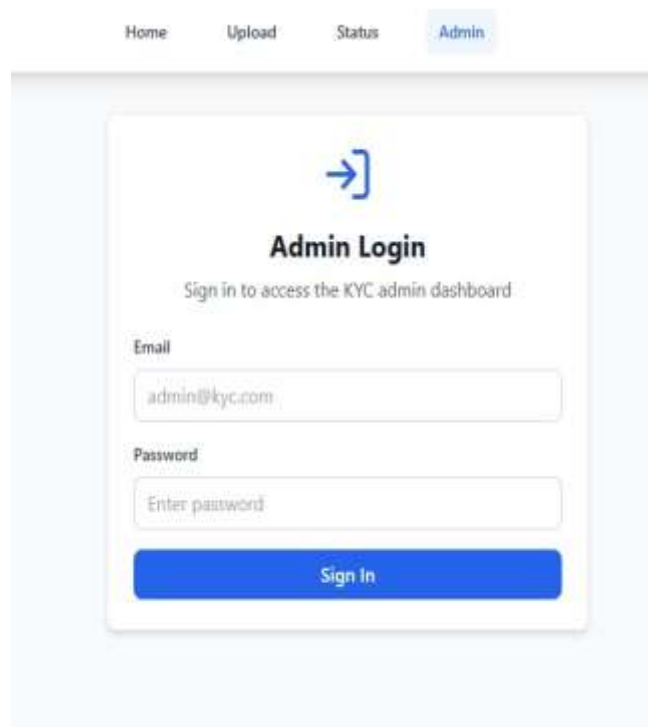
II. Experimental Setup and Observations

Prototype deployed to Polygon Mumbai testnet. Typical observations: average IPFS pin latency 1–2 seconds, average transaction confirmation 2–5 seconds on testnet, and modest gas usage for storing small strings (CIDs).

C. Comparison Table

TABLE I
TRADITIONAL VS BLOCKCHAIN-BASED KYC (QUALITATIVE)

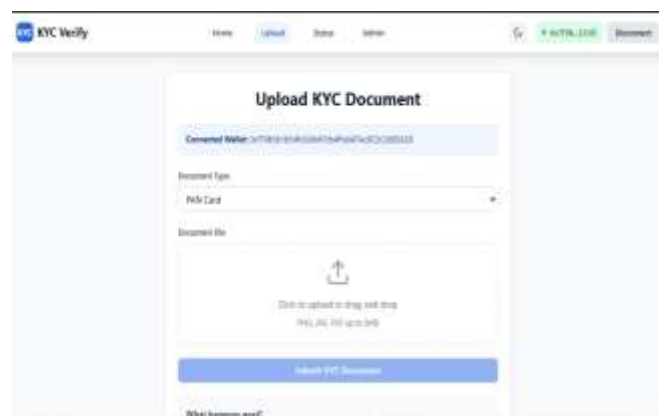
Feature	Traditional KYC	Blockchain KYC
Data storage	Centralized DB	Off-chain + on-chain hashes
Tamper-proof	No	Yes (on-chain)
Redundancy	High	Low
User control	Low	Higher (self-sovereign)
Cost	Variable, recurring	Transaction costs (one-time anchors)
Privacy risk	High	Reduced (if encrypted)



SECURITY AND PRIVACY ANALYSIS

The methodology incorporates strict security measures to protect sensitive data. All customer information is encrypted before storage, ensuring confidentiality. Smart contracts enforce role-based access control, preventing unauthorized usage. By using blockchain's decentralized nature, the system eliminates risks associated with central databases, thereby enhancing resilience against data breaches and cyberattacks.

The methodology adopts a structured and iterative approach to design and implement a blockchain-based KYC verification system. By utilizing Ethereum, smart contracts, and decentralized storage, combined with Agile development practices, the project ensures a secure, efficient, and user-friendly solution. The methodology not only addresses existing challenges in KYC verification but also lays a foundation for future enhancements and large-scale adoption in the financial sector.



LIMITATION AND FUTURE WORK

Limitations include dependency on testnet behavior for performance metrics, possible availability concerns for IPFS, and regulatory acceptance barriers. Future work: integrate DIDs and Verifiable Credentials (W3C), explore ZKP-based attribute proofs, batch anchoring using Merkle trees, and evaluate enterprise-grade deployments.

One of the major limitations of the current implementation is the scalability of the Ethereum blockchain. As the number of KYC requests increases, transaction delays and high gas fees can hinder performance. Future work could involve integrating Layer-2 scaling solutions such as Optimistic Rollups or zk-Rollups to handle a larger volume of transactions more efficiently. Alternatively, migrating to next generation blockchains like Polkadot, Cardano, or Hyperledger Fabric could provide better scalability and lower costs for enterprise adoption.

For real-world adoption, interoperability with existing financial systems and regulatory platforms is essential. Future work could focus on designing APIs and middleware to integrate the blockchain-based KYC framework with banking systems, government identity platforms, and international compliance networks. This would enable seamless sharing of verified identities across institutions, reducing redundancy and further lowering costs.

The current project demonstrates the feasibility of using blockchain and smart contracts for KYC verification, but significant opportunities remain for expansion and improvement. By addressing scalability, enhancing security, enabling interoperability, and ensuring regulatory compliance, the system can evolve into a widely adopted solution for global identity management. With continued research and

development, blockchain-based KYC has the potential to revolutionize not only financial services but also a wide range of sectors that rely on trusted identity verification.

ACKNOWLEDGEMENTS (OPTIONAL)

If you wish to identify funding sources or significant contributions by others, please include your acknowledgements at the end of your paper but before the References. **Only include this information on the final camera-ready copy.**

CONCLUSION

The project began with an exploration of the challenges associated with traditional KYC verification, including inefficiency, high costs, and vulnerability to fraud and data breaches. To address these issues, blockchain technology was identified as a promising solution due to its decentralization, immutability, and cryptographic security. The research then focused on designing a secure and user-friendly KYC verification framework using the Ethereum blockchain and smart contracts.

The system was designed with three key roles—Admin, Organization, and Customer—each supported by well-defined workflows enforced through smart contracts. Customer data was encrypted and stored on IPFS to ensure privacy, while only hash values were recorded on the blockchain for verification. An interactive website was developed to provide role-based dashboards, enabling seamless interaction between stakeholders and the blockchain system.

In conclusion, this research successfully demonstrated the design and implementation of a blockchain-based KYC verification system. By combining Ethereum smart contracts, decentralized storage, and an interactive web interface, the system addressed key challenges of traditional KYC processes. The outcome is a secure, transparent, and efficient verification framework that enhances trust among stakeholders.

REFERENCES

1. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," <https://bitcoin.org/bitcoin.pdf>, 2008.
2. 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.61 048–61 073, 2021.
3. Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.
4. V. Buterin, "Ethereum white paper: A next-generation smart contract and decentralized application platform," <https://ethereum.org/en/whitepaper/>, 2014.
5. G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," *Ethereum Project Yellow Paper*, 2014.
6. N. Szabo, "Smart contracts: Building blocks for digital free markets," [https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart contracts 2.html](https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart%20contracts%20.html), 1996.
7. N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (sok)," in *Proceedings of the 6th International Conference on Principles of Security and Trust*, 2017, pp. 164–186.
8. M. C. Lacity, *A Manager's Guide to Blockchain for Business*. Cutter Consortium, 2018.
9. V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamar 1a, "Blockchain and smart con-

- tracts for insurance: A review,” *Future Internet*, vol. 10, no. 2, p. 7, 2018.
10. 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.
 11. S. Nazarov, S. Ellis, and A. Juels, “Chain-link: A decentralized oracle network,” <https://link.smartcontract.com/whitepaper>, 2017.
 12. S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, and Y. Guo, “Blockchain-powered parallel healthcare systems based on the acp approach,” *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1131–1143, 2019.
 13. C. M. E. Tschupp and S. M. Lorenz, “Etherisc: A decentralized insurance protocol,” White Paper, 2018. [14] H. Karp, “Nexus mutual: A decentralized alternative to insurance,” White Paper, 2019.
 14. C. Oham, R. Jurdak, S. S. Kanhere, A. Dorri, and S. Jha, “B-fica: Blockchain-based framework for auto insurance claim and adjudication,” *IEEE Transactions on Engineering Management*, 2024.
 15. P. Varalakshmi, B. Sivasankari, R. A. Kumar, K. M. N. Kumar, and T. V. Venkhan, “Development of healthcare insurance claim mechanism using blockchain technology,” in *2022 1st International Conference on Computational Science and Technology (ICCST)*, 2022, pp. 835–839.
 16. Y. Farooqui and S. M. Parikh, “Secure and transparent supply chain management using blockchain and iot,” *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 4, pp. 123–135, 2023.
 17. S. Agal, K. M. Raulji, Y. Farooqui, N. Bhavsar, and R. Agrawal, “Innovative financial services driven by ai and blockchain synergy for decentralized trust and personalized solutions,” in *2024 IEEE 2nd International Conference on Innovations in High-Speed Communication and Signal Processing (IHCSP)*, 2024, pp. 1–8.
 18. S. Shi, Q. Wang, Z. Zhang, and X. Chen, “A survey on blockchain scalability: Issues, solutions, and challenges,” *IEEE Access*, vol. 9, pp. 21 409–21 429, 2021.
 19. C. Gorenflo, S. Lee, L. Golab, and S. Keshav, “Fastfabric: A lightweight and scalable blockchain for high-performance Dapps,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 1, pp. 57–69, 2021.
 20. M. Zamani, M. Movahedi, and M. Raykova, “Rapidchain: A fast and scalable bft protocol for blockchains,” in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 97–112.
 21. PricewaterhouseCoopers, “Global insurance report 2020: Taming complexity and unlocking value,” 2020.
 22. Coalition Against Insurance Fraud, “The state of insurance fraud 2023,” 2023.
 23. X. Shi, W. Zhang, and L. Wang, “A survey on blockchain technology for healthcare,” *IEEE Access*, vol. 9, pp. 160 816–160 835, 2021.
 24. W. Li, S. Andreina, J. Bohli, and G. Karame, “Securing proof-of-stake blockchain protocols,” *International Journal of Security Studies*, pp. 1257–1270, 2020.
 25. Y. Farooqui, D. Patel, M. Kumar, R. Mehta, and R. Vyas, “Towards a decentralized future: The role of deverse in publishing evolution,” in *2024 Parul International Conference on Engineering and Technology (PICET)*, 2024, pp. 1–6.
 26. L. Zhou, L. Wang, and Y. Sun, “Mistore: A blockchain-based medical insurance storage system,” *Journal of Medical Systems*, vol. 42, p. 149, 2021.