Zero Knowledge and IPFS Based Know Your Customer (KYC)

Sachin Prasanna
Information Technology
NIT Karnataka
Surathkal, India
211IT058

Abhayjit Singh Gulati
Information Technology
NIT Karnataka
Surathkal, India
211IT085

Abstract—**The Know Your Customer (KYC) process is essential for institutions to verify client identities, yet traditional methods often incur high costs and pose privacy risks. This paper explores how blockchain technology, with its decentralization and immutability, can enhance the KYC process by improving security and reducing costs. Additionally, it highlights the use of Zero-Knowledge Proofs (ZKPs) as a privacy-preserving solution, allowing identity verification without revealing sensitive information. By integrating ZKPs with blockchain, the paper offers a framework for more secure, efficient, and private KYC systems.**

I. Introduction

In the modern financial landscape, institutions such as banks and corporations serve a diverse and extensive clientele across both retail and corporate sectors. A crucial element of this interaction is the 'Know Your Customer' (KYC) process, which enables these institutions to verify the identity of their clients. KYC compliance is not only a regulatory requirement but also a legal obligation that financial entities must adhere to for both new and existing customers. However, the KYC process presents a significant challenge in the form of escalating regulatory costs, which place a financial burden on institutions striving to meet compliance standards [1].

Traditionally, financial institutions have relied on conventional KYC methods to perform identity verification [2]. However, these methods often involve centralized systems, which may compromise privacy, introduce inefficiencies, and incur high operational costs. The advent of blockchain technology offers a potential solution to these challenges, thanks to its inherent characteristics of decentralization, immutability, and trustlessness [1]. By leveraging these attributes, blockchain can enhance the security and integrity of the KYC process while reducing the need for intermediaries.

Blockchain's appeal lies in its ability to provide security, anonymity, and data integrity without relying on a central authority. This decentralized approach not only ensures the transparency and integrity of transactions but also opens new avenues for research, particularly in addressing the technical challenges and limitations associated with privacy-preserving verification methods [3].

Among these emerging methods, Zero-Knowledge Proofs (ZKPs) offer distinct advantages. ZKPs allow one party to prove the validity of certain information without revealing the information itself, making them particularly suited for privacy-sensitive environments like KYC. Compared to other cryptographic techniques such as homomorphic encryption and secure multiparty computation, ZKPs stand out for their minimal security assumptions and broad applicability. Their potential to ensure confidential verification across various domains, including blockchain-based KYC, has sparked significant interest in both academia and industry [4].

II. Literature Review

Blockchain is a decentralized, continuously growing ledger of records validated by network participants. Initially developed for managing cryptocurrency transactions, blockchain's distributed ledger technology has expanded into various domains, including healthcare [5]. Its decentralized architecture relies on peer-to-peer (P2P) networks, cryptographic techniques, and consensus algorithms to ensure secure and transparent data storage without the need for central authorities [6].

The key advantages of blockchain technology—decentralization, immutability, and traceability—make it ideal for systems requiring high security and integrity. These features have led to its use in building tamper-resistant data storage solutions and in designing privacy-preserving transactions, enabling secure interactions between parties without revealing sensitive information [7].

In the process of enrolling new customers or updating existing ones, KYC has become a crucial requirement for institutions such as banks and insurance companies to verify their clients' involvement in any illegal activities [8]. However, the current KYC process faces several challenges that create inefficiencies for both customers and organizations. These include Human Error, Lack of Skilled Personnel, Malicious Users, Duplication and Costs, Time Delays, Reputational and Regulatory Risks, Lack of International Standards [9]

To address the challenges of traditional KYC processes, the concept of utilizing blockchain technology for KYC has emerged. Malhotra et al. [2] propose a solution where financial institutions implement KYC using a private blockchain. In this approach, a client's identity is verified only once, and the verified information is securely stored on the blockchain. This allows other financial institutions to access the stored data for future verification, eliminating the need for repeated KYC checks.

In the approach given by Yadav et al. [1] after the details provided by the user are authenticated, all the data provided by the user in the KYC form is then added into the Blockchain. They use the Ethereum API for building the Blockchain using solidity language to create a smart contract. The user is then notified that his/her details have been verified and he/she can now proceed to apply to banks where he/she wishes to open an account. The user will be presented a list of banks wherein which he/she simply has to tap on the list item of that bank.

To further enhance KYC security, Zero-Knowledge Proofs (ZKP) can be utilized. ZKPs allow users to prove possession of certain information without disclosing the information itself, offering an additional layer of privacy [10]. The application of ZKPs on the blockchain has gained popularity recently. For example, Partala et al. review various ZKP schemes applied to confidential transactions and private smart contracts on blockchains [11]. Li et al. propose a decentralized, privacy-preserving architecture that integrates ZKPs into blockchain-based traffic management systems to ensure data integrity and privacy [12].

In addition, we will leverage InterPlanetary File System (IPFS) to efficiently store and share large files. IPFS uses cryptographic hashes, which can be easily stored on a blockchain. [13].

III. Problem Statement

In a traditional KYC (Know Your Customer) process, users need to provide sensitive personal information such as name, address, and date of birth to service providers like banks, insurance companies, or government agencies. This data is typically stored in centralized databases, raising concerns about privacy, data breaches, and unauthorized access. Furthermore, service providers often require specific information (e.g., verifying that a person is over 18 or resides in a certain country), but not the full details of the person's identity or address. The challenge is to create a system that allows users to prove certain facts about themselves (e.g., age, residence) without revealing sensitive information.

IV. Objectives

A. Data Privacy and Security

Implementing a decentralized KYC system using Zero-Knowledge Proofs (ZKPs) to ensure that users can prove their attributes (e.g., age, residency) without revealing their full personal details. Sensitive data is encrypted and stored on the InterPlanetary File System (IPFS), ensuring privacy and protection from unauthorized access.

B. Decentralized and Immutable Storage

Utilizing blockchain technology to record cryptographic proofs of KYC updates and changes, ensuring that no centralized authority can alter the records. This creates a tamper-proof, auditable ledger for KYC compliance, enabling transparency and accountability.

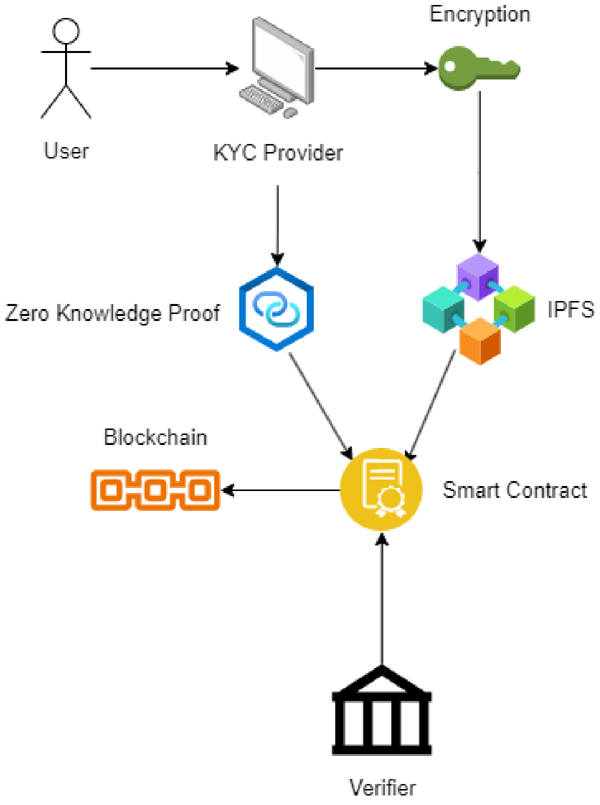

Fig. 1. Proposed Architecture

C. Efficient Verifiability

Enabling service providers to verify specific claims about a user's identity or attributes through Zero-Knowledge Proofs, without accessing the full KYC data. The blockchain provides a secure and automated method for verification, significantly reducing manual checks and maintaining privacy.

V. Architecture

Figure 1 illustrates the architecture of our proposed decentralized KYC system, integrating Zero-Knowledge Proofs (ZKPs), IPFS, and blockchain. The architecture ensures secure, private, and verifiable KYC data management.

A. User Device and Input

The user initiates the KYC process through their device, entering personal data such as name, date of birth, address, and other identity-related information. The data is first encrypted using the user's private key, ensuring that sensitive information is protected from unauthorized access.

B. IPFS Storage

The encrypted KYC data is stored in the InterPlanetary File System (IPFS). The IPFS system provides decentralized storage, ensuring that the data remains accessible even in the absence of a centralized server. The system generates a unique content identifier (CID) for the stored data, which can be used to retrieve the data when needed.

C. Blockchain Ledger

The CID generated from IPFS is recorded on the blockchain. This immutable ledger ensures that once the KYC data is uploaded and verified, the proof of the KYC and any changes made to it are permanently stored, making the system tamper-proof and auditable.

D. Zero-Knowledge Proofs (ZKP) Verification

Service providers can request specific information from the user without accessing the full KYC data. This speeds up the process greatly. Using ZKPs, the user can prove these attributes without revealing the underlying sensitive information. The blockchain is leveraged to validate these ZKPs, ensuring that the verification process is secure and efficient.

E. Smart Contracts

Smart contracts govern the rules for data verification and sharing. Once a ZKP verification request is made by a service provider, the smart contract checks the conditions and interacts with the blockchain to ensure that the necessary proofs are valid, without compromising the user's privacy.

F. Administrator and Regulatory Role

An administrative authority (optional) can monitor and regulate KYC processes. Their role includes overseeing policy compliance and ensuring that the system adheres to relevant regulatory requirements.

References

[1] P. Yadav and R. Chandak, "Transforming the know your customer (kyc) process using blockchain," in *2019 International Conference on Advances in Computing, Communication and Control (ICAC3)*, pp. 1–5, 2019.

[2] D. Malhotra, P. Saini, and A. K. Singh, "How blockchain can automate kyc: Systematic review," *Wireless Personal Communications*, vol. 122, no. 2, pp. 1987–2021, 2022.

[3] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," *PloS one*, vol. 11, no. 10, p. e0163477, 2016.

[4] R. Lavin, X. Liu, H. Mohanty, L. Norman, G. Zaarour, and B. Krishnamachari, "A survey on the applications of zero-knowledge proofs," *arXiv preprint arXiv:2408.00243*, 2024.

[5] A. A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, "Blockchain vehicles for efficient medical record management," *NPJ digital medicine*, vol. 3, no. 1, p. 1, 2020.

[6] R. Johari, V. Kumar, K. Gupta, and D. P. Vidyarthi, "Blosom: Blockchain technology for security of medical records," *ICT Express*, vol. 8, no. 1, pp. 56–60, 2022.

[7] S. Ma, Y. Deng, D. He, J. Zhang, and X. Xie, "An efficient nizk scheme for privacy-preserving transactions over account-model blockchain," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 641–651, 2020.

[8] P. C. Mondal, R. Deb, and M. N. Huda, "Transaction authorization from know your customer (kyc) information in online banking," in *2016 9th international conference on electrical and computer engineering (ICECE)*, pp. 523–526, IEEE, 2016.

[9] W. M. Shbair, M. Steichen, J. François, *et al.*, "Blockchain orchestration and experimentation framework: A case study of kyc," in *IEEE/IFIP Man2Block 2018-IEEE/IFIP Network Operations and Management Symposium*, 2018.

[10] P.-W. Chi, Y.-H. Lu, and A. Guan, "A privacy-preserving zero-knowledge proof for blockchain," *IEEE Access*, vol. 11, pp. 85108–85117, 2023.

[11] J. Partala, T. H. Nguyen, and S. Pirttikangas, "Non-interactive zero-knowledge for blockchain: A survey," *IEEE Access*, vol. 8, pp. 227945–227961, 2020.

[12] W. Li, H. Guo, M. Nejad, and C.-C. Shen, "Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach," *IEEE access*, vol. 8, pp. 181733–181743, 2020.

[13] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, "Blockchain-based, decentralized access control for ipfs," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 1499–1506, 2018.