Zero Knowledge and IPFS Based Know Your Customer

IT465 Course Project

Sachin Prasanna : 211IT058
Abhayjit Singh Gulati : 211IT085

Under the Guidance of
Dr. Bhawana Rudra, Assistant Professor

Dept. of Information Technology
National Institute of Technology Karnataka, Surathkal

September 27, 2024

Overview

Introduction

- **KYC Importance:** Essential for institutions to verify client identities, ensuring regulatory compliance.
- **Challenges:** Traditional KYC methods incur high costs, pose privacy risks, and rely on centralized systems.
- **Blockchain Solution:** Offers decentralization and immutability, enhancing security and reducing operational costs.
- **Zero-Knowledge Proofs (ZKPs):** Enable identity verification without revealing sensitive information, suitable for privacy-sensitive environments.
- **Research Potential:** ZKPs' broad applicability and minimal security assumptions make them a promising solution for efficient, secure, and private KYC systems.

Literature Survey

- **Malhotra et al. :** Proposed a solution for implementing KYC using a private blockchain where a client's identity is verified only once, and the verified information is securely stored for future access by financial institutions.
- **Yadav et al. :** Developed an approach where authenticated KYC details are added to the blockchain using Ethereum API and Solidity. Users are notified upon verification and can easily apply to banks.
- **Partala et al. :** Reviewed various Zero-Knowledge Proof (ZKP) schemes applied to confidential transactions and private smart contracts on blockchains, highlighting the benefits of privacy.
- **Li et al. :** Proposed a decentralized, privacy-preserving architecture integrating ZKPs into blockchain-based traffic management systems to ensure both data integrity and privacy.
- **General KYC Challenges:** Addressed by the need for blockchain technology in KYC processes to overcome issues such as human error, lack of skilled personnel, and time delays.

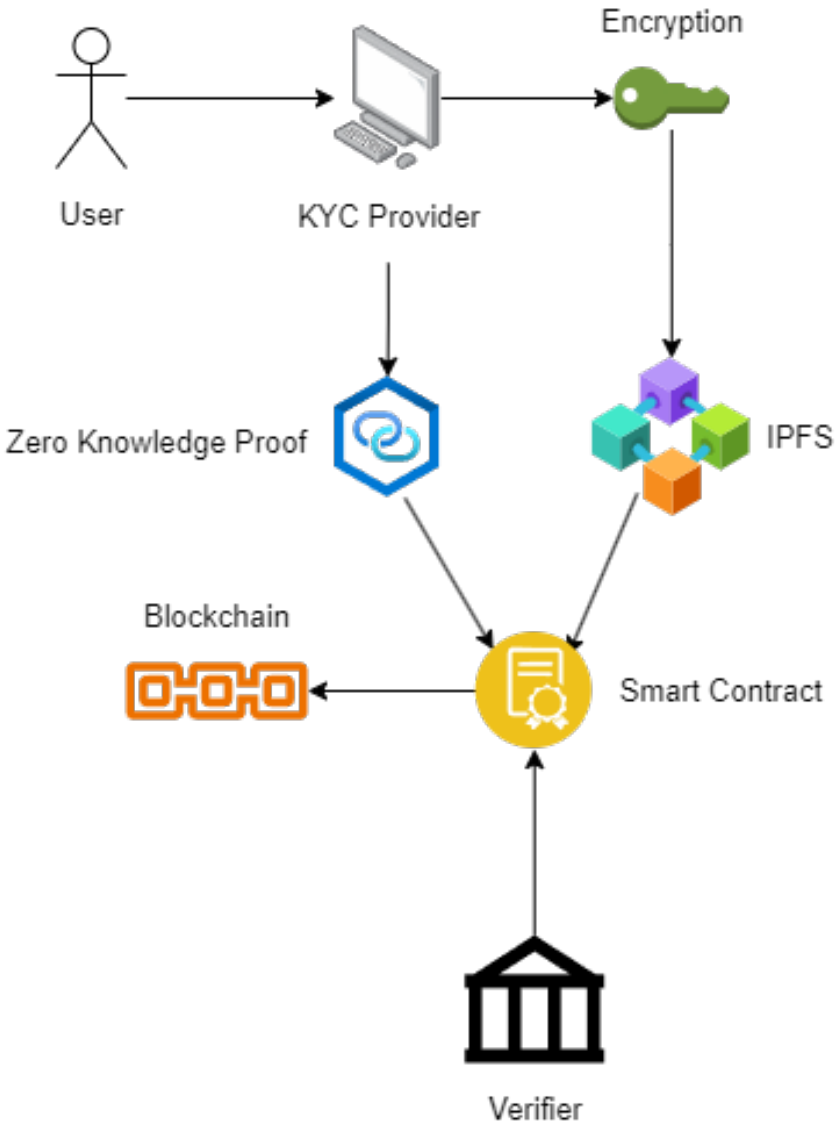
Problem Statement

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.

Objectives

- **Data Privacy and Security:**
  - Implement a decentralized KYC system using Zero-Knowledge Proofs (ZKPs).
  - Ensure users can prove attributes without revealing full personal details.
  - Store sensitive data encrypted on IPFS for privacy and protection.
- **Decentralized and Immutable Storage:**
  - Use blockchain to record cryptographic proofs of KYC updates.
  - Ensure no centralized authority can alter records.
  - Create a tamper-proof, auditable ledger for KYC compliance.
- **Efficient Verifiability:**
  - Enable service providers to verify user attributes via ZKPs.
  - Reduce manual checks through secure, automated blockchain verification.
  - Maintain privacy while ensuring fast and efficient verifiability.

Architecture



Technology Stack

- **Solidity**: A programming language used for writing smart contracts on the Ethereum blockchain, enabling secure and decentralized logic for KYC processes.
- **Remix IDE**: An open-source web and desktop application used for developing, testing, and deploying Solidity smart contracts efficiently.
- **Python**: A versatile programming language used for writing scripts that interact with the blockchain and execute Zero-Knowledge Proofs (ZKPs) for verification without revealing personal data. It will also be used to take input from the user for the KYC.
- **Ganache**: A personal Ethereum blockchain for local development that allows for the testing of smart contracts and simulates the behavior of a real blockchain environment.
- **MetaMask**: A cryptocurrency wallet and gateway to blockchain applications that enables users to manage their identities and interact securely with the decentralized application.
- **Pinata API**: A service that simplifies the process of storing and managing files on the InterPlanetary File System (IPFS), allowing for the secure and decentralized storage of KYC data.

Thank You