A Digital Fingerprint on Solana Blockchain

Abstract

There are many use cases associated with Blockchain Technology like finance, NFT, Domain services, payments etc. But almost everything on Blockchain is done anonymously with hexadecimal or some type of encoded cryptographic strings (public keys). This has proven to be secure as well as it helps in hiding one's identity from going public. But in some Applications users are required to do KYC, provide their identity in order to use some applications. In this case we need a protocol which can automatically fetch data from Blockchain with user's permission and prove their identity and still provide privacy support for users so that their data is not public on-chain by encrypting their data. This is the problem we are trying to solve.

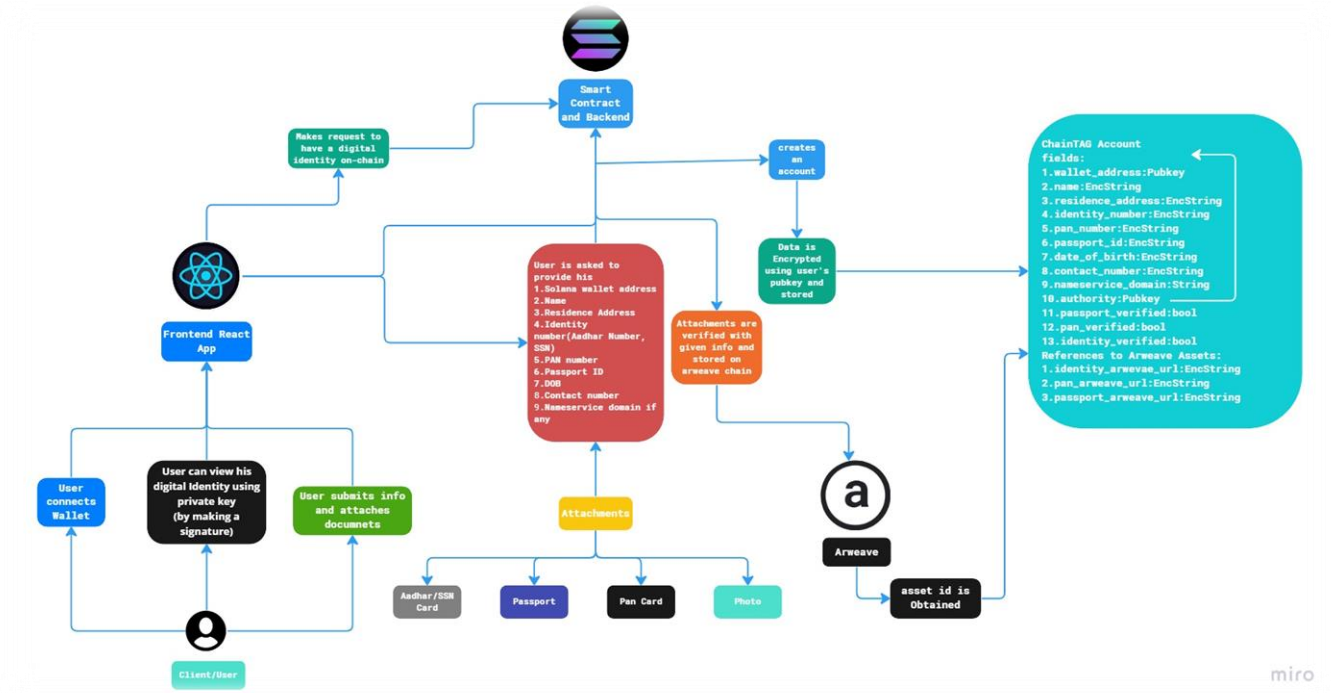
Objectives

1. Create a secure platform where users can use the protocol to create their digital identity on-chain by providing their info like (Wallet address, Name, Ph No, Residential Address, Identity document numbers like aadhaar, passport , Social Security Number etc.
2. Create a storage service to store identity proof as attachments like Photo, Aadhaar, PAN and Passport.
3. Write Smart Contracts to create Accounts on Solana with all the given information by users and Encrypt them while storing them. This provides privacy of user information on-chain.
4. Setting the Account's authority as respective users so that they have the sole power to modify, delete and permit application to view raw data.
5. Verifying the attachments with the information provided by users to prove legitimacy of data.

Applications

1. This protocol can be used in doing KYC.
2. In trading , payments we can verify parties involved
3. In various agreements like (rental, property, assets) which reside on Blockchain.
4. NFT ownership verification
5. Verifying participants in an event.

Design



How is this different from Web2 Solution?

1. Web2 is centralized (data availability can be compromised) which is addressed by Blockchain.
2. Web2 works on OTP and passwords which can be compromised but our application works on Wallet connect and Cryptographic encryption and decryption algorithms to access raw data.
3. In Web2 data is stored on centralized storages and it can be attacked to retrieve data. This is addressed by using Arweave (a decentralized storage Blockchain which is secure and stores any form of data efficiently.
4. User owns his data which gives them authority to modify, delete and permit access for others whenever he wants.

Team

Nagaprasad V.R (1SI19CS085)

Harshavardhan T.K (1SI19CS048)

Akshay H.N (1SI19CS008)

Sagar Hemanth (1SI19CS101)