Project Report

Decentralized Digital Identity Verification System using Blockchain

1. Introduction

Identity verification plays a crucial role in accessing government services, banking, education, healthcare, and many digital platforms. Traditionally, identity data such as Aadhaar, PAN, or passports are stored in large centralized databases managed by institutions. However, centralized systems are vulnerable to data breaches, unauthorized access, misuse of personal records, and identity theft.

To address these concerns, this project presents a **Decentralized Digital Identity System** built using **Blockchain** and **IPFS (InterPlanetary File System)**. Instead of storing the actual documents on servers, documents are stored in a decentralized storage network (IPFS), and only a **reference hash (CID)** is stored on the blockchain. The blockchain maintains the verification status, ensuring transparency, immutability, and tamper resistance.

Users interact with the system using **MetaMask**, giving them complete ownership of their digital identity. An authorized verifier reviews identity submissions and approves or rejects based on authenticity.

2. Problem Statement

Centralized identity verification systems face the following limitations:

- **Risk of Data Breach:** A single hack can cause exposure of millions of identities.
- **Lack of Transparency:** Users cannot see how their identity is processed or stored.
- **No Ownership:** Users rely on third-party institutions to validate their identity.
- **Manual Verification is Slow:** Verification processing is often time-consuming.

Thus, there is a need for a **secure, transparent, decentralized, and user-controlled identity verification system**.

3. Objectives

The primary objectives of this project are:

- **Ensure Data Security:** Store documents in decentralized storage to prevent tampering.
- **Guarantee Transparency:** Track identity verification workflow through smart contracts.
- **User Ownership:** Allow users to control identity using their blockchain wallet.
- **Verifier Authorization:** Ensure only authorized verifier accounts can approve identities.
- **Minimal On-Chain Storage:** Store only IPFS CIDs on blockchain to reduce storage cost.

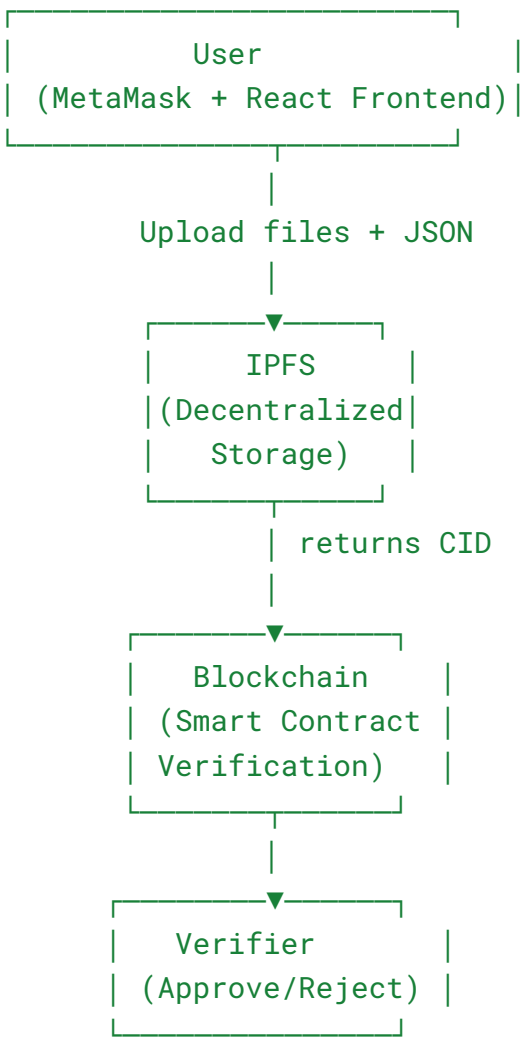
4. Literature & Existing Solutions

Existing identity systems include:

System	**Limitation**
Government Portals	Centralized, single point of failure
Private KYC Vendors	Expensive and opaque
Cloud-stored digital vaults	Vulnerable to unauthorized access
Centralized Databases	Lack transparency and user control

Blockchain-based identity management has emerged as a secure alternative, but many solutions still store data on-chain, increasing cost and privacy issues. Our solution separates **storage (IPFS)** and **verification logic (Blockchain)**, making it lightweight and practical.

5. System Architecture



6. Technology Stack

Layer	Technology Used
Frontend UI	React.js, HTML, CSS
Blockchain	Hardhat, EVM Local Node
Smart Contract	Solidity
Wallet Authentication	MetaMask
Storage	IPFS (Local Node)
Interaction	ethers.js Web3 library

7. Smart Contract Design

Data Structure

Each identity is stored as:

```
struct Identity {
    string cid;         // IPFS CID of identity JSON
    Status status;       // PENDING / VERIFIED / REJECTED
}
```

Workflow

User Action	Contract Effect
Submit identity	CID stored, status → PENDING
Verifier Approves	Status → VERIFIED
Verifier Rejects	Status → REJECTED
User Checks Status	CID + Status returned

Role Separation

- **User:** Any wallet holder.
- **Verifier:** Only contract deployer (admin account).

8. Implementation Workflow

For User

1. Connect wallet via MetaMask.
2. Enter personal details (name, date of birth, address).
3. Upload Aadhaar and PAN files.
4. System:
    - Uploads documents to **IPFS**
    - Creates identity JSON

    - Uploads JSON to IPFS
    - Submits CID to smart contract
5. User waits for verification.

For Verifier

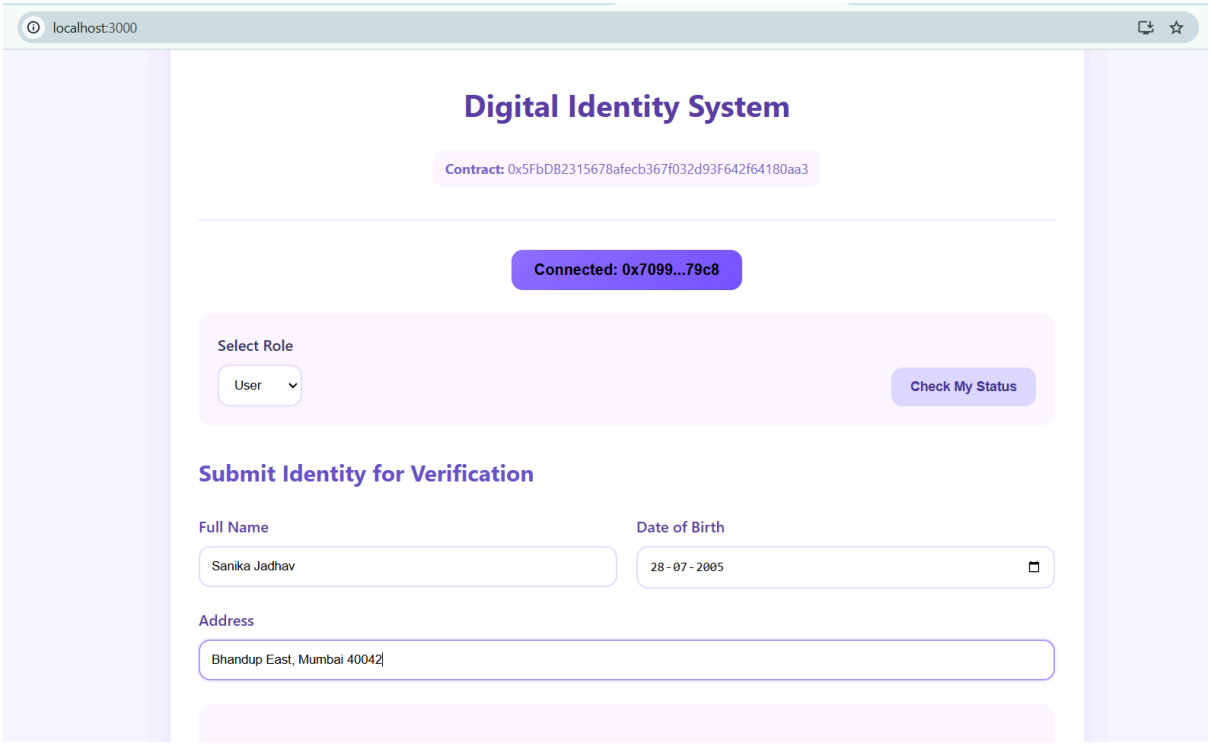
1. Switch to verifier wallet.
2. Open dashboard → Load pending applicants.
3. View identity details + documents (Aadhar/PAN).
4. Approve or Reject.
5. Status updates on blockchain.

9. Results

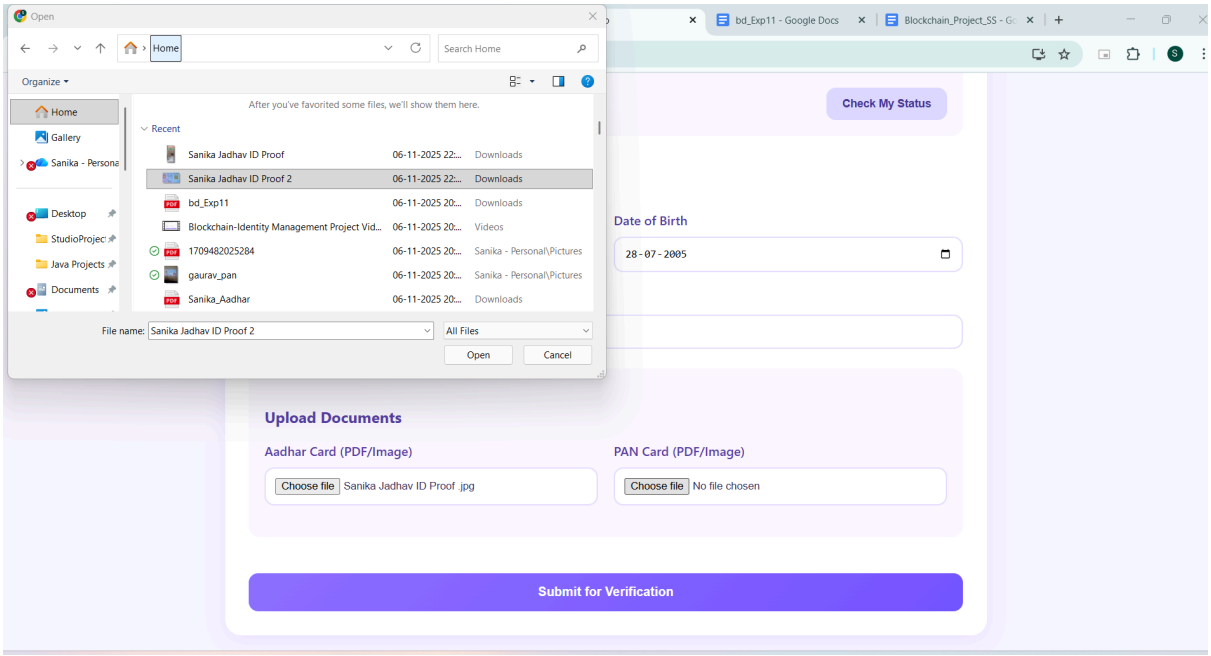
Feature	**Outcome**
Data Security	Ensured by IPFS content-addressing
Transparency	Blockchain verification traceability
User Ownership	Wallet-based identity control
Privacy	Only CID is on-chain, not files
Verification Efficiency	One-click approval/rejection by verifier

10. Screenshots

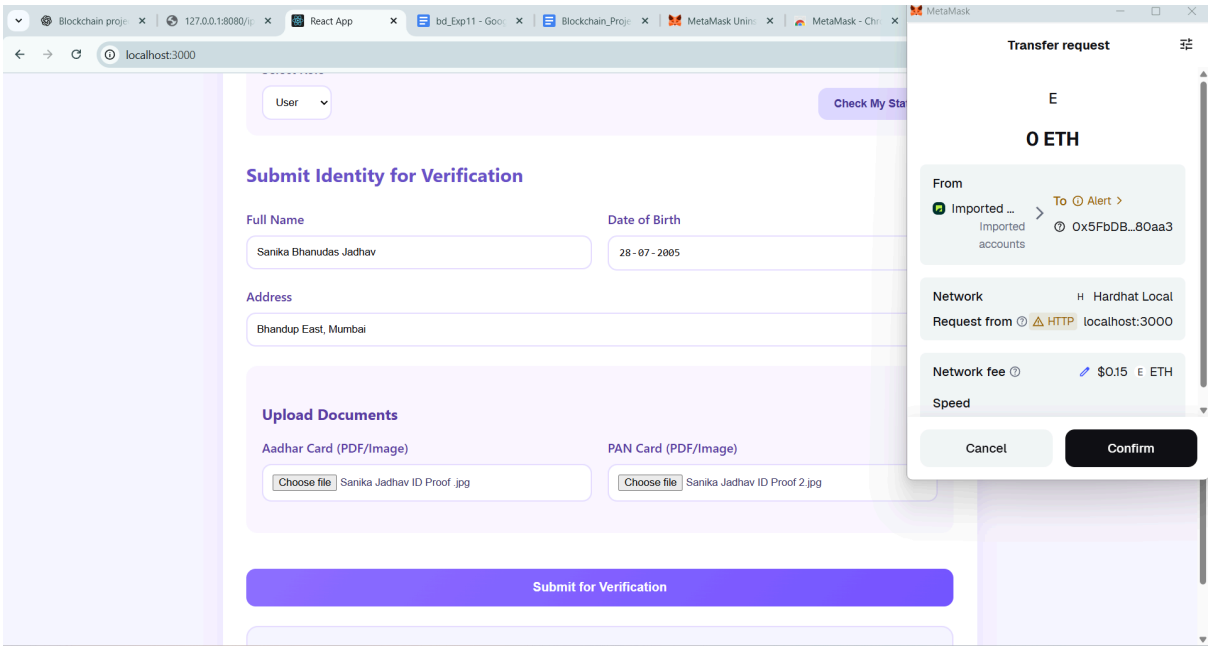
1.User Panel



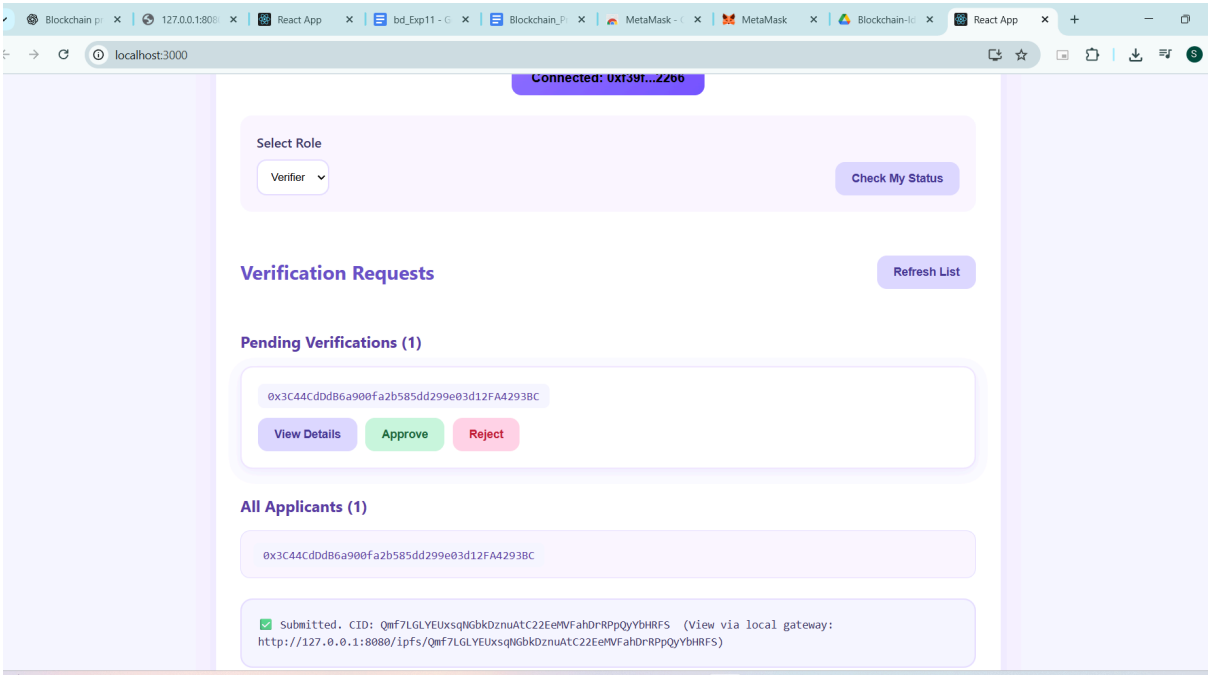
2.User Enters Details & Uploads Documents For Verification



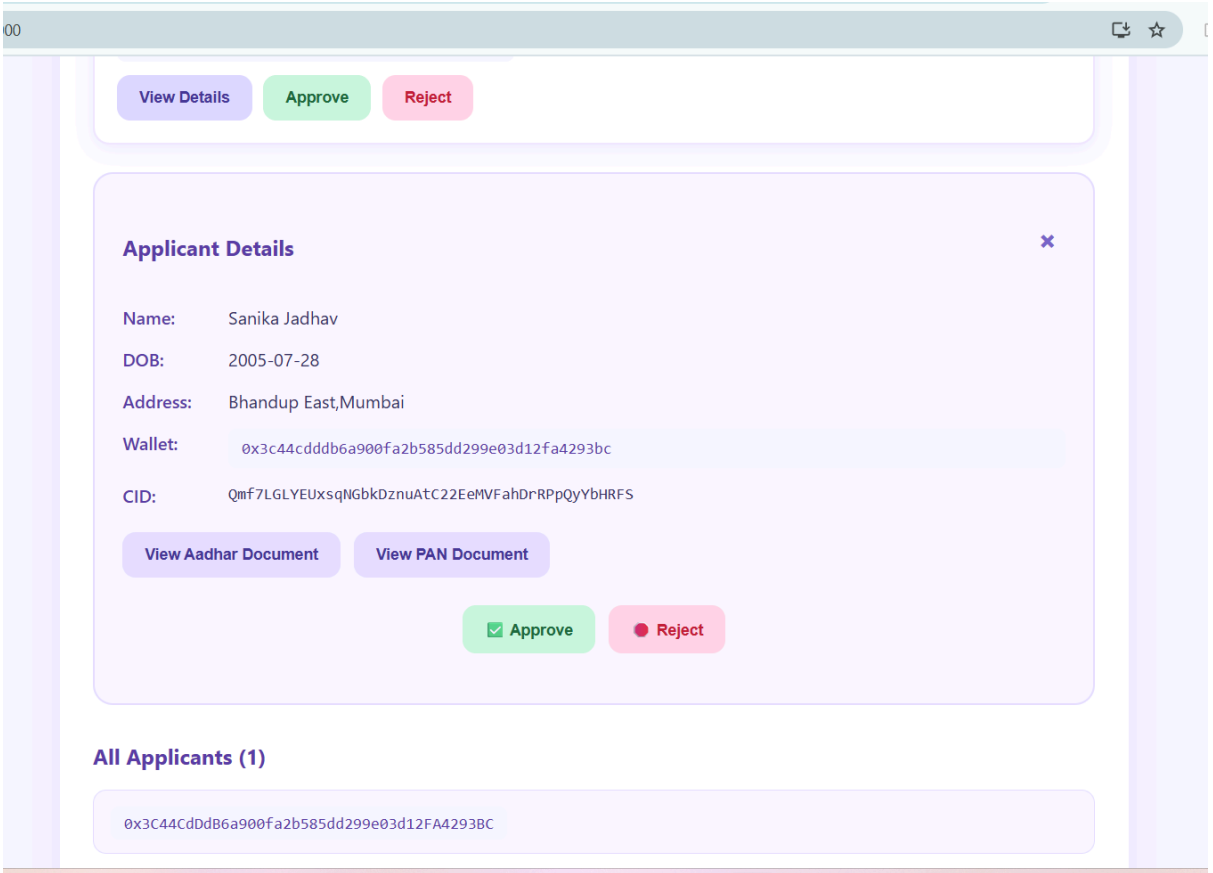
3.Pay Transaction Fee to submit

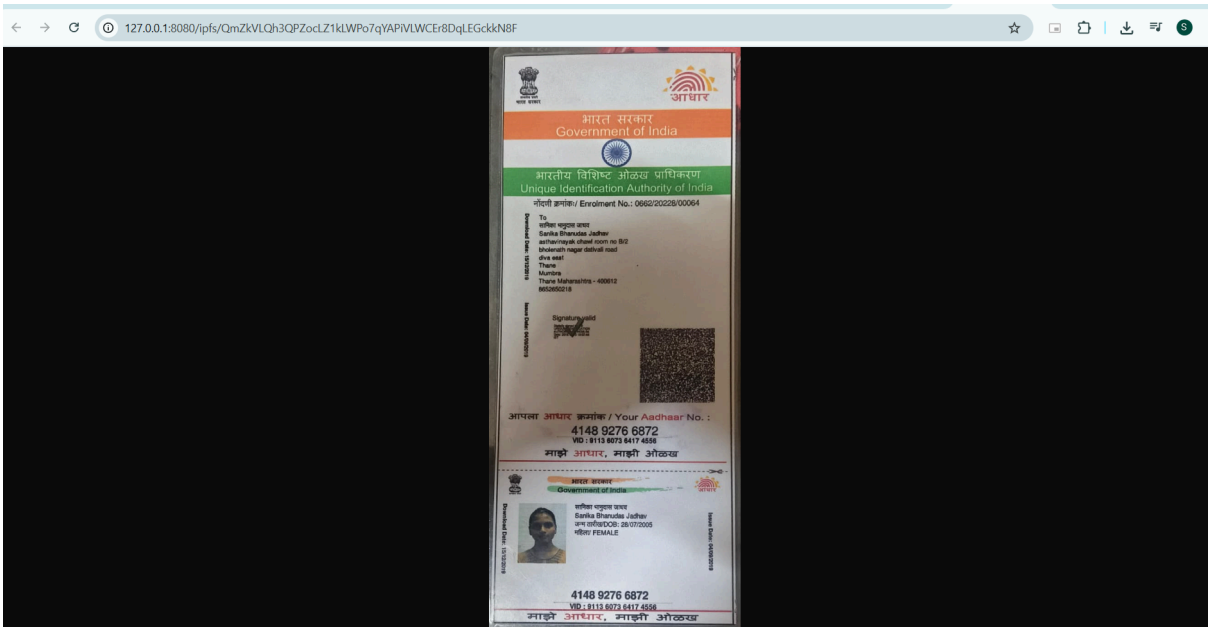


4.Verifier Panel

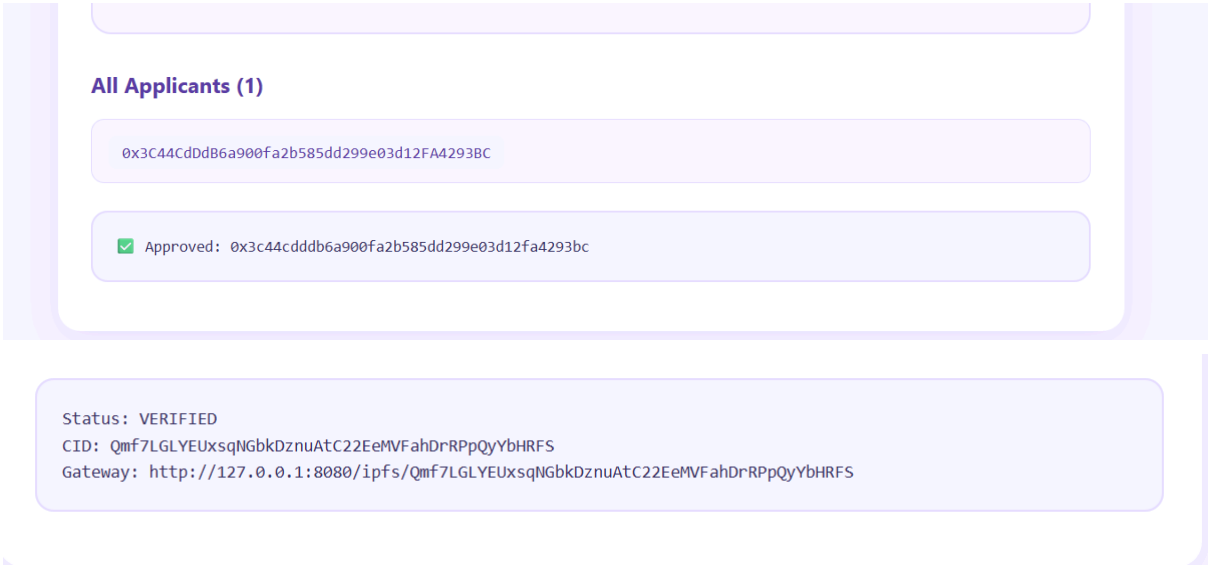


5.Verifier Checks Submitted Details and Documents for Identity Creation





6.Verifier approves the request



11. Conclusion

This project demonstrates a **secure and decentralized model for identity verification**. By leveraging blockchain for verification and IPFS for document storage, it ensures tamper resistance, transparency, and user control over identity. The system removes reliance on centralized authorities and enhances data integrity.