IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, February 2026
Impact Factor: 8.2

Decentralized Trust Verification System

Ms.Snehal Pagare[1], Kalyani Warule[2], Mrunalini Sonawane[3], Sakshi Patil[4], Harshada Pingale[5]
Hod, Department of Information Technology[1]
Students, Department of Information Technology[2,3,4,5]
Mahavir Polytechnic, Nashik, Maharashtra, India

Abstract: *In the digital era, identity verification plays a crucial role in online services such as banking, healthcare, education, and government applications. Traditional identity management systems rely on centralized authorities that store sensitive user data, making them vulnerable to data breaches, identity theft, and unauthorized access. This paper proposes a Decentralized Identity Verification System (DID) based on blockchain technology that enables secure, transparent, and usercontrolled identity management. The proposed system utilizes blockchain networks and smart contracts to store encrypted identity records, ensuring immutability and privacy. Users maintain control over their identity credentials while institutions can verify authenticity without accessing sensitive personal data. The decentralized architecture eliminates dependency on centralized authorities and enhances trust, privacy, and security in digital identity verification.*

Keywords*:* Blockchain, Digital Identity, Decentralized Identity (DID), Smart Contracts, Cybersecurity

I. INTRODUCTION

Digital identity verification has become essential for accessing online services. Conventional identity systems depend on centralized databases maintained by organizations such as government agencies, banks, or service providers. These centralized systems create single points of failure, increasing the risk of data breaches and identity theft. Additionally, users often lose control over their personal information once it is stored in centralized systems.

Blockchain technology provides a decentralized and tamper-resistant infrastructure that enables secure identity management without relying on centralized authorities. By using blockchain and smart contracts, identity credentials can be securely stored, verified, and shared with authorized entities while maintaining privacy. The proposed decentralized identity verification system allows users to create and manage their digital identities securely while enabling organizations to verify identity authenticity efficiently.

A Decentralized Document Verification System is a blockchain-based web application designed to securely store, verify, and validate documents such as educational certificates, identity proofs, legal papers, and employment records. The system ensures authenticity, prevents forgery, and provides transparency by using blockchain technology where records are immutable and tamper-proof. The Decentralized Document Verification System uses blockchain technology to ensure data integrity, transparency, security, real-time verification, reduced paperwork, and faster processing while preventing fraud and data manipulation.

II. LITERATURE SURVEY

Zyskind, G., Nathan, O., & Pentland, A. — Decentralizing Privacy: Using Blockchain to Protect Personal Data (2018)- Document verification is critical in academic, legal, and business environments. Traditional centralized systems often suffer from data tampering, fraud, and lack of transparency. Blockchain technology offers immutable, secure storage, enabling trustworthy verification systems. This literature survey discusses past research, existing solutions, and how blockchain-based verification systems have evolved.

DOI: 10.48175/IJARSCT-31358

III. IMPLEMENTATION OF THE DECENTRALIZED IDENTITY VERIFICATION SYSTEM

The Decentralized Identity Verification System (DID) is implemented using blockchain technology to provide secure, tamper-proof, and user-controlled identity management. The implementation integrates blockchain networks, smart contracts, web interfaces, and cryptographic mechanisms to ensure secure identity registration and verification.

A. System Architecture

The system follows a decentralized client–blockchain architecture where:

The user application (web/mobile interface) acts as the client layer for identity registration and management.

The blockchain network (Ethereum / Hyperledger) stores identity hashes and verification transactions.

Smart contracts manage identity creation, authentication, and verification processes.

Off-chain storage systems (IPFS / MongoDB) store encrypted identity data while maintaining references on the blockchain.

This architecture ensures data immutability, transparency, and decentralized control over identity records.

B. Front-End Implementation

The front-end interface is developed using modern web technologies such as HTML, CSS, JavaScript, and React.js. The user interface provides functionalities including:

User registration and login

Identity creation and credential management

Verification request submission

Viewing verification status and transaction history

The interface communicates securely with blockchain nodes using APIs and wallet integrations such as MetaMask.

C. Smart Contract Implementation

Smart contracts are developed using Solidity and deployed on the blockchain network. These contracts perform key operations such as:

Generating unique decentralized identity identifiers (DIDs)

Storing encrypted identity hashes

Handling verification requests

Recording verification results on the blockchain

Smart contracts ensure automation, transparency, and tamper-proof identity verification.

D. Backend and Database Integration

Backend services are implemented using Node.js and Express.js to handle authentication, API requests, and interaction with blockchain nodes. Off-chain databases such as MongoDB or IPFS store encrypted user identity information to improve scalability while blockchain stores only verification references and transaction logs.

E. Security and Privacy Implementation

The system applies cryptographic techniques such as hashing, digital signatures, and encryption to secure identity data. Public–private key mechanisms ensure that only authorized users can access or share their identity credentials. Multi-factor authentication and secure wallet authentication mechanisms enhance user security.

F. Deployment and Testing

The decentralized identity system is deployed on a blockchain test network to evaluate system functionality and performance. Testing includes unit testing for smart contracts, integration testing for system modules, and user acceptance testing to validate usability and security. Continuous monitoring ensures system reliability and scalability.

DOI: 10.48175/IJARSCT-31358

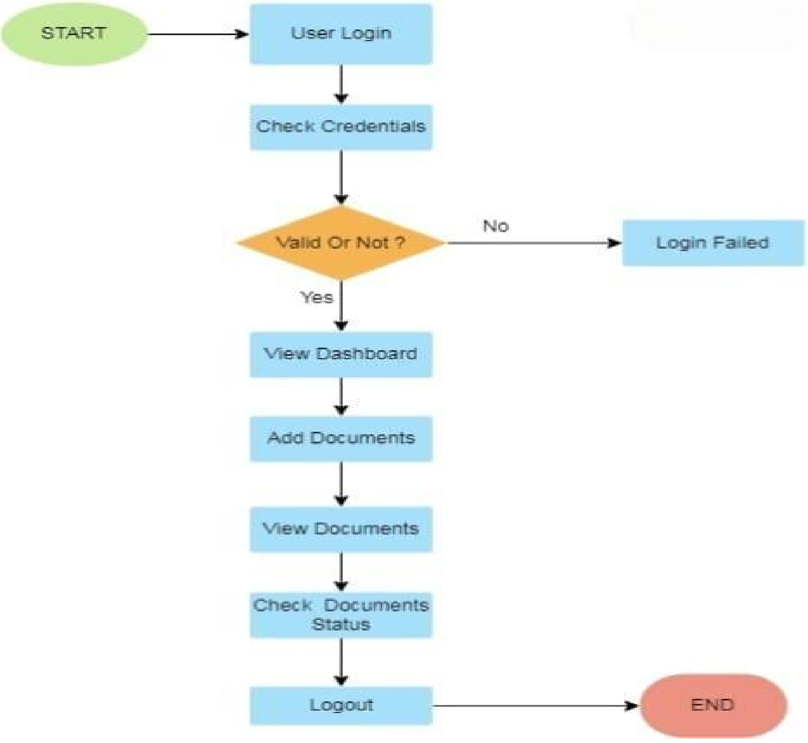

Fig 1. User Login Flow

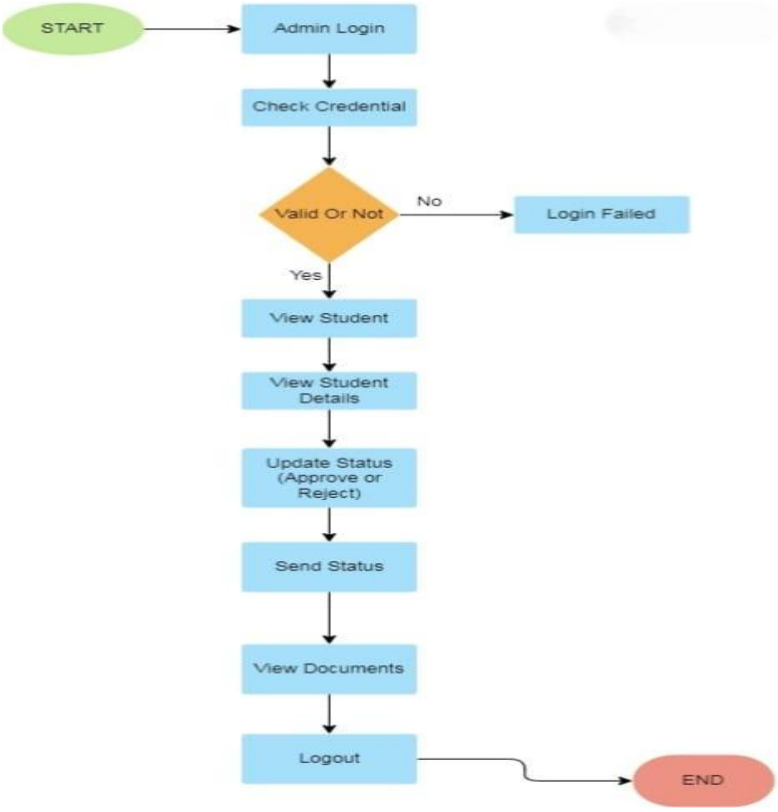

Fig 2. Admin Flow

DOI: 10.48175/IJARSCT-31358

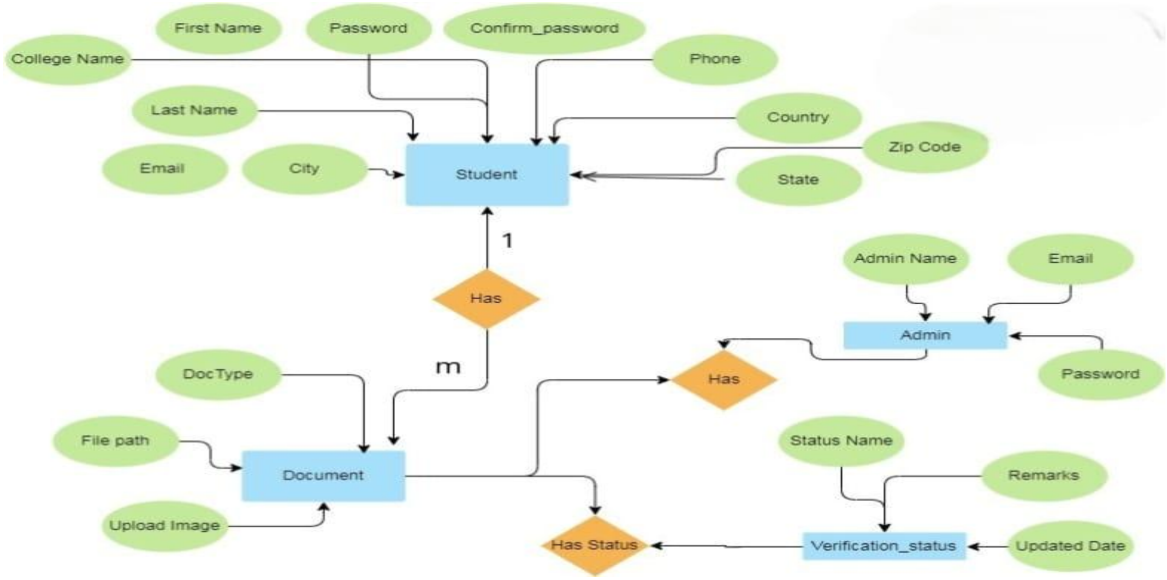

Fig 3. Working Flow

IV. FUTURE WORK

In the future, the Decentralized Identity Verification System can be enhanced by integrating biometric authentication such as fingerprint or facial recognition to improve security. Mobile identity wallets can be developed to allow users to store and manage their identity credentials conveniently. The system can also support interoperability between multiple blockchain networks and integration with government, banking, healthcare, and educational platforms for large-scale adoption. Additionally, advanced privacy techniques such as zero-knowledge proofs and AI-based fraud detection mechanisms can be incorporated to further improve privacy, security, and reliability of the identity verification process.

V. CONCLUSION

The proposed Decentralized Identity Verification System provides a secure, transparent, and efficient solution for managing digital identities using blockchain technology. By eliminating dependency on centralized authorities and implementing smart contract-based verification, the system ensures data integrity, privacy, and tamper-proof identity management. The platform enables users to maintain control over their personal information while allowing organizations to verify identities quickly and reliably. Overall, the system enhances trust, security, and efficiency in digital identity verification and has strong potential for adoption across sectors such as education, banking, healthcare, and government services.

VI. ACKNOWLEDGMENT

We would like to express our sincere gratitude to our project guide and faculty members for their valuable guidance, continuous support, and encouragement throughout the development of this project. We are also thankful to our department and institution for providing the necessary resources and technical facilities required to complete this work successfully. Finally, we extend our appreciation to our team members, friends, and family for their cooperation, motivation, and support during the entire project development process.

REFERENCES

[1]. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[2]. W3C, “Decentralized Identifiers (DIDs) v1.0,” 2022.

[3]. Hyperledger Foundation, “Hyperledger Indy Documentation,” 2021.

[4]. Ethereum Foundation, “Smart Contracts and Decentralized Applications,” 2023

DOI: 10.48175/IJARSCT-31358