www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1748-1752

e-ISSN : 2583-1062
Impact Factor : 7.001

DIGITAL IDENTITY VERIFICATION – A BLOCKCHAIN-BASED SYSTEM FOR VERIFYING AND MANAGING DIGITAL IDENTITIES

Diksha Sanjay Gurav[1], Shreya Ramkrishna Gurav[2], Anushka Sanjay Mate[3], Mayuri Mahendra Kumbhar[4], Prof. Vijay B. Mohite[5]

[1,2,3,4,5]Computer Engineering, Zeal Polytechnic, Pune, India.

ABSTRACT

In today's digital age, identity verification is crucial for secure access to services across finance, governance, and healthcare. However, traditional identity systems are often centralized, creating single points of failure that are vulnerable to breaches, identity theft, and privacy violations. This paper proposes a blockchain-based solution for digital identity verification, emphasizing decentralization, transparency, and user ownership. By leveraging smart contracts and cryptographic techniques, the proposed system allows users to control their identity data while enabling verifiable credentials and secure access. Developed as an Android application, the system integrates with blockchain wallets and uses smart contracts to manage and verify identities without relying on intermediaries. It also critically examines the limitations of blockchain-based ID systems and outlines future development opportunities to support large-scale adoption. The prototype demonstrates feasibility on Android, enabling DID generation and QR-based identity sharing in a secure manner.

Keywords: Blockchain Technology, Smart Contracts, Digital Identity Verification, Decentralization, Privacy Preservation, Identity Management, User-Centric Identity, Big Data, Network Trust

1. INTRODUCTION

In today's digitally connected world, the rapid pace of technological advancement has made it clear how critical secure identity verification has become across various sectors. With the expansion of online services in finance, healthcare, education, and governance, traditional identity systems struggle to meet the demands for privacy, control, and security. Centralized systems, while widely used, are increasingly vulnerable to data breaches and identity theft. At the same time, users expect seamless and secure access to services without compromising personal data. According to recent research, the global push towards decentralized systems is gaining momentum, with blockchain expected to play a key role in shaping future digital infrastructures. Identity verification, once a static and repetitive process, now demands automation, transparency, and user empowerment—principles that blockchain technology is uniquely equipped to deliver.

2. OBJECTIVES

The primary objective of the Digital Identity Verification system is to develop a blockchain-based solution that enhances security, privacy, and user control in digital identity management. The system aims to eliminate the vulnerabilities of centralized identity systems through decentralization, ensuring trustless and secure identity verification. Specific objectives include:

1. **Decentralizing Identity Management**: To develop a system that eliminates the need for centralized databases, allowing users to control and manage their identity data securely using blockchain technology.
2. **Enhancing Privacy and Security**: To implement cryptographic techniques, such as encryption and digital signatures, to ensure that identity data remains secure and tamper-proof.
3. **Verifiable Credentials**: To enable users to issue and present verifiable credentials, ensuring that digital identity information can be shared in a trusted and transparent manner with third-party verifiers.
4. **User Empowerment**: To design a Self-Sovereign Identity (SSI) system that allows individuals to manage and share their identity data selectively, providing them with full control over their personal information.
5. **Seamless Blockchain Integration**: To integrate the system with blockchain wallets, allowing users to manage their digital identities efficiently without relying on intermediaries.

BACKGROUND:

Digital identity verification has become a critical component in securing access to online services, including banking, healthcare, and government services. Traditional identity systems rely on centralized models, creating vulnerabilities such as data breaches and unauthorized access. Blockchain technology, with its decentralized, immutable nature, offers a promising alternative by ensuring data privacy, security, and user autonomy.

Recent advancements in blockchain have led to the development of Self-Sovereign Identity (SSI) systems, which empower individuals to control their identity data without depending on central authorities. According to a 2023 report

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1748-1752
e-ISSN : 2583-1062
Impact Factor : 7.001

by the World Economic Forum, blockchain-based identity solutions are poised to revolutionize digital identity verification, offering secure and transparent alternatives to traditional systems.

Key concepts in this field include decentralized identifiers (DIDs), which allow users to create and manage unique digital identifiers on a blockchain, and verifiable credentials, which provide tamper-proof proof of identity. Solutions like Estonia's e-Residency program and Switzerland's digital identity initiative demonstrate how blockchain can streamline public services and increase trust in digital interactions.

3. LITERATURE SURVEY

Traditional identity verification systems have historically relied on centralized databases, which pose significant risks of data breaches and lack transparency [1], [8]. These systems are inherently vulnerable to single-point failures, often resulting in massive data leaks and unauthorized access to user information.

The introduction of blockchain technology by Nakamoto [2] laid the foundation for decentralized systems, offering tamper-resistance, transparency, and auditability. Blockchain's ability to enhance the security and privacy of digital identities is further supported by research that explores its application in securing big data and protecting user information from unauthorized access [3], [6]. By utilizing blockchain, digital identity systems can establish trust and safeguard sensitive data in a decentralized environment, addressing critical security concerns that arise in traditional, centralized systems.

Recent research has shifted toward Decentralized Identity (DID) frameworks, which empower users to manage their identities independently without relying on a central authority. The W3C's DID specification defines how these identities can be created, resolved, and verified securely [4].

Verifiable credentials, as explored by Mastorocostas et al. [5], are a key element in blockchain-based identity systems, enabling users to prove specific attributes without exposing complete identity details. This selective disclosure maintains privacy while supporting trust and verification. While these systems present significant advantages in terms of privacy and security, further exploration is needed in the areas of scalability and user adoption, as some challenges remain unresolved in existing solutions.

4. GAPS IDENTIFIED IN EXISTING SYSTEM

While traditional and even some modern digital identity verification systems have evolved significantly, several key challenges and limitations remain unaddressed. Existing solutions often:

- Rely on centralized architecture, creating single points of failure that are prone to data breaches and cyberattacks.
- Lack user control over personal data, leading to privacy concerns and non-compliance with data protection regulations like GDPR.
- Depend heavily on third-party intermediaries for verification, increasing the risk of data manipulation and delays.
- Struggle with interoperability across platforms and lack support for secure, portable, and reusable identities.

Solutions to Identified Gaps:

Our proposed blockchain-based identity verification system overcomes existing limitations by introducing a decentralized, secure, and transparent approach to managing digital identities. It removes the need for centralized data storage by anchoring identity-related proofs on the blockchain, enhancing trust and reducing the risk of tampering. Through smart contracts, the system automates verification processes, minimizing the reliance on intermediaries. Users maintain control over their identity through integration with blockchain wallets, aligning with the principles of self-sovereign identity.

5. PROPOSED SYSTEM

5.1 System Overview:

The proposed system is a blockchain-based decentralized identity verification platform that leverages blockchain technology, smart contracts, and verifiable credentials to manage and verify digital identities securely. The system ensures user control, privacy, and compliance with data protection regulations like GDPR.

5.2 Features:

DID Creation: Users can generate a decentralized identifier (DID) stored on a blockchain.

QR Code Generator: A unique QR code representing the user's identity is generated, allowing secure, one-click sharing.

Wallet Integration: The app connects to a blockchain wallet for identity data management.

User Autonomy: Users can update and revoke their identity data directly through the app.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1748-1752

e-ISSN : 2583-1062
Impact Factor : 7.001

5.3 Modules:

Identity Management Module: Allows users to generate, store, and manage their decentralized identities (DIDs) on the blockchain.

Admin/Service Module (optional): For services to scan and retrieve identity info for trustless verification (not currently implemented, but open for future expansion).

5.4 System Architecture:

The Android app communicates with a blockchain network to store and retrieve user DIDs. The system uses smart contract interactions for secure identity data anchoring and generates QR codes linked to the DID.

A user-friendly app interfaces with blockchain wallets for seamless identity management.

5.5 Activity flow:

User inputs identity information → App generates DID on blockchain → DID is encoded into QR code → QR code is displayed and can be scanned for identity reference.

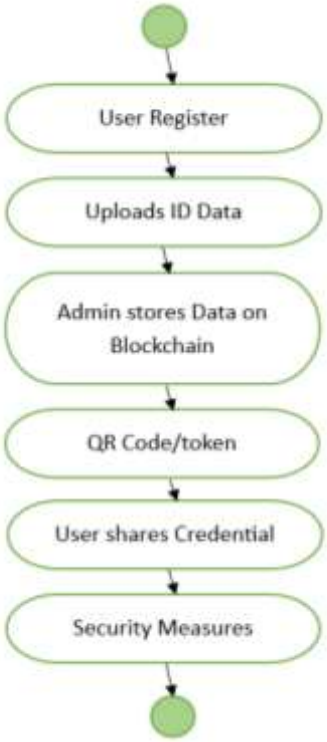

Fig 1. Activity diagram

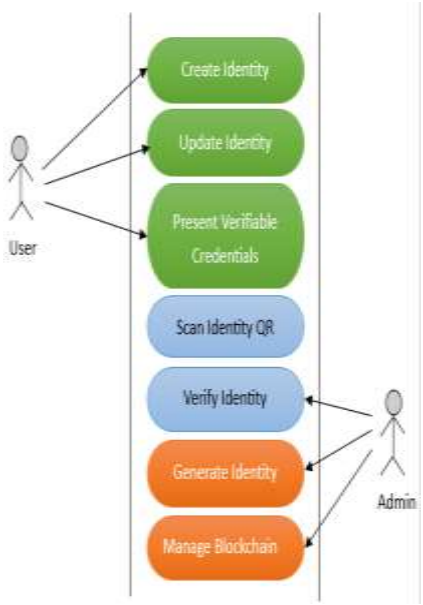

Fig 2. Use Case Diagram

www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 1748-1752
e-ISSN : 2583-1062
Impact Factor : 7.001

6. IMPLEMENTATION

6.1. Algorithm for Implementing a Blockchain-based Decentralized Identity System:

1. Develop Decentralized Identity Framework:

• Set up a blockchain network supporting DID standards (e.g., W3C DID).

• Create a system where users generate and own their DIDs with minimal intermediaries.

• Build a user-friendly app for managing DIDs, enabling users to control and update their identity data.

2. Design Verifiable Credentials Infrastructure:

• Implement a mechanism for trusted authorities to issue cryptographically secure credentials (e.g., licenses, certificates).

• Build a validation process allowing third parties to verify credentials without accessing full identities, using cryptographic techniques.

3. Integrate Smart Contracts:

• Develop and deploy smart contracts to automate identity verification based on pre-set conditions (e.g., age, nationality).

• Automate credential validation and manage exceptions (e.g., expired credentials).

4. Enhance Privacy and Compliance:

• Implement Zero-Knowledge Proofs (ZKPs) to verify attributes without revealing personal data.

• Ensure GDPR compliance by giving users control over their identity data, with options for revocation and consent-based sharing.

5. Integrate with Regulations and Legacy Systems:

• Collaborate with regulators to meet legal requirements and overcome barriers.

• Develop APIs or middleware to integrate the blockchain system with legacy systems (e.g., banking, healthcare). 6. Pilot and Testing:

• Pilot the system in sectors with high identity verification needs (e.g., finance, healthcare).

• Test system reliability across various devices and environments, addressing any vulnerabilities.

7. User Education and Adoption:

• Educate users on secure digital identity management through campaigns and resources.

6.2. Tools and Technology:

Frontend Platform: Android

Backend Platform: Kotlin (integrated within Android app)

Smart Contract Language: Solidity

Blockchain Framework: Ethereum

Blockchain Wallet Integration: MetaMask (for signing transactions)

Blockchain Connector: Web3j

OCR Integration: Google ML Kit

Biometric Authentication: Android Biometric API

QR Code Handling: QRGen (Android)

Data Storage:

Off-Chain: Firebase / IPFS / Database

7. CONCLUSION

This blockchain-based digital identity system offers a secure, decentralized alternative to traditional verification methods. By combining QR code generation, smart contracts, and self-sovereign identity principles, it empowers users with control over their data while ensuring trust and transparency. With future enhancements like biometric integration and cross-platform support, the system holds strong potential for real-world adoption across sectors.

8. REFERENCES

[1] Z. Song, G. Wang, Y. Yu, and T. Chen, “Digital identity verification and management system of blockchain-based verifiable certificate with the privacy protection of identity and behavior,” in Proc. IEEE, 2022.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[3] F. Wang, Y. Gai, and H. Zhang, "Blockchain user digital identity big data and information security process protection based on network trust," IEEE Access, vol. 8, pp. 156-165, 2020.

[4] W3C, "Decentralized identifiers (DIDs) v1.0," World Wide Web Consortium (W3C), 2020. [Online]. Available: https://www.w3.org/TR/did-core/.

[5] P. Mastorocostas, M. K. Kaur, and M. M. P. M. Zohar, "Blockchain-based verifiable credentials for privacy-preserving identity management," IEEE Access, vol. 9, pp. 101093–101106, 2021.

[6] G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing privacy: Using blockchain to protect personal data,” in Proc. IEEE Security and Privacy Workshops (SPW), 2015.

[7] A. Preukschat and D. Reed, Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials. Manning Publications, 2021.

[8] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, “A survey on essential components of a self-sovereign identity,” Future Generation Computer Systems, vol. 81, pp. 706–722, 2018.