IDentix: Blockchain-Based Decentralized Identity Verification System

Swaraj Chikhale, Shantanu Chimote, Rakshit Sinha, Swaraj Rathod, Gaurang Bhasme ,Prof. S. P. Palaskar
Department of Information Technology
Sipna College Of Engineering And Technology-Amravati
Email: swarajchikhale2004@gmail.com, shantanuchimote42@gmail.com, rakshitsinha1474@gmail.com, swarajrathod32@gmail.com, gaurangbhasme@gmail.com

***Abstract*— Traditional identity systems rely on centralized authorities, which creates single points of failure and privacy risks. We propose *IDentix*, a decentralized identity framework leveraging blockchain and cryptography to secure user credentials while preserving privacy. In IDentix, each user owns a self-sovereign identity (SSI) represented by a public/private key pair and a Decentralized Identifier (DID) registered on an Ethereum smart contract. Trusted issuers (e.g. governments, banks) provide verifiable credentials (VCs) to users off-chain, and users present cryptographic proofs (such as zero-knowledge proofs) of specific attributes to verifiers. Verifiers authenticate credentials by checking issuer signatures against public keys on the blockchain and querying an immutable credential registry. Our prototype on the Ethereum Sepolia testnet demonstrates that this design yields tamper-evident identity proofs without exposing personal data. As shown in prior work [1], blockchain-based SSI greatly reduces risks of identity theft while giving users full control over their data.**

Keywords— Blockchain; decentralized identity; self-sovereign identity; verifiable credentials; decentralized identifiers; identity verification; Ethereum; zero-knowledge proof.

I. INTRODUCTION

Identity verification plays a fundamental role in secure digital ecosystems, especially in sectors such as education, finance, and e-governance. Traditional identity verification infrastructures typically depend on centralized database systems that store user credentials and personal records within a single administrative authority. Although these systems are widely used, they introduce several security and trust challenges. Centralized databases can become attractive targets for cyberattacks, resulting in large-scale data breaches and identity theft incidents. Additionally, administrators with privileged access may intentionally or unintentionally modify stored records, which compromises the integrity of identity information.

Recent studies highlight that centralized identity systems lack transparency and auditability, making it difficult to detect unauthorized modifications to identity data [1]. Furthermore, traditional authentication methods such as static identification cards or fixed QR codes are vulnerable to replay attacks, where attackers reuse captured authentication credentials to gain unauthorized access.

Blockchain technology has emerged as a promising solution for addressing these issues. A blockchain is a distributed ledger that stores transactions in an immutable and tamper-resistant manner. Once data are recorded on the blockchain, they cannot be modified without network consensus, which provides strong guarantees of data integrity and transparency [2]. Because of these characteristics, blockchain platforms have been increasingly explored for identity management applications.

Another emerging concept is Self-Sovereign Identity (SSI), which allows individuals to control and manage their own identity credentials without relying entirely on centralized authorities. In SSI systems, identity proofs can be verified using cryptographic techniques while maintaining user privacy [3]. Blockchain technology can act as a trust layer for SSI systems by securely storing identity references, hashes, or verification metadata.

Motivated by these developments, this research proposes IDentix, a blockchain-based decentralized identity verification system designed for institutional environments such as universities or organizations. Instead of storing full identity data on the blockchain, the proposed system stores cryptographic hashes of identity records, while the detailed user data remain stored in a secure database. This hybrid

architecture combines the efficiency of traditional databases with the immutability of blockchain networks.

The IDentix system also introduces dynamic QR-based authentication, where a time-dependent cryptographic hash is embedded in a QR code generated within a mobile application. The QR code automatically expires after a short time interval, thereby preventing replay attacks and ensuring that authentication tokens cannot be reused.

The main contributions of this work include:

- Design of a blockchain-integrated identity verification framework using Ethereum Sepolia.
- Implementation of a dynamic QR authentication mechanism for secure real-time verification.
- Development of a hybrid architecture combining MongoDB data storage with blockchain-based integrity validation.
- Experimental evaluation using real-world institutional data to demonstrate system effectiveness.

The remainder of this paper is organized as follows. Section II reviews related work in blockchain-based identity systems. Section III describes the methodology of the proposed system. Section IV presents the system architecture. Section V explains the implementation and evaluation results. Finally, Section VI concludes the paper and outlines potential future improvements.

II. LITERATURE SURVEY

Recent advancements in blockchain technology have encouraged researchers to explore decentralized approaches for identity management. Traditional identity systems rely heavily on centralized authorities to store and verify identity records. While these systems are widely deployed, they introduce issues such as lack of transparency, vulnerability to cyberattacks, and risks of unauthorized data modification. Consequently, researchers have proposed blockchain-based identity frameworks to improve trust and security.

Zyskind et al. proposed one of the early decentralized identity management models using blockchain technology, demonstrating how distributed ledgers can provide secure control over personal data without relying on centralized intermediaries [1]. Their work highlighted that blockchain networks can act as trusted platforms where identity records can be verified while maintaining user privacy.

Later, Tobin and Reed introduced the concept of Self-Sovereign Identity (SSI), where individuals manage their digital identities independently and selectively disclose personal attributes to service providers [2]. SSI architectures typically rely on decentralized identifiers (DIDs) and verifiable credentials, which allow identity attributes to be validated without revealing sensitive information.

Several researchers have also explored the use of blockchain in financial identity verification systems. Thadari and Kumar proposed a blockchain-based identity verification mechanism for digital banking environments. Their work demonstrated that storing identity verification proofs on blockchain networks improves resistance against impersonation and man-in-the-middle attacks [3]. The study showed that blockchain immutability can significantly enhance the reliability of identity validation systems.

Similarly, Li et al. introduced a distributed identity management system that combines blockchain with cryptographic authentication mechanisms. Their framework provides secure identity registration, authentication, and revocation processes through smart contracts deployed on blockchain networks [4]. The research emphasizes that decentralized identity infrastructures can reduce dependence on centralized databases.

Another important aspect of identity verification is privacy preservation. Salah et al. proposed a blockchain-based identity system for electronic healthcare cards where zero-knowledge proofs are used to verify user attributes without revealing sensitive personal data [5]. This work demonstrates how cryptographic techniques can strengthen privacy protection in decentralized identity platforms.

Despite these advancements, many existing systems require complete identity information to be stored directly on the blockchain, which may increase storage costs and raise privacy concerns. Additionally, several solutions rely on static authentication tokens, which remain vulnerable to replay attacks.

To address these limitations, the proposed IDentix system introduces a hybrid architecture where complete identity records are stored in a secure database, while cryptographic hashes of identity records are stored on the blockchain. This approach preserves privacy while still leveraging the immutability of blockchain technology. Furthermore, the system integrates dynamic QR-based

authentication, which generates time-limited verification tokens to prevent replay attacks.

III. METHODOLOGY

The IDentix system follows a hybrid decentralized architecture that integrates blockchain technology with a conventional database infrastructure to achieve secure identity verification. The methodology focuses on maintaining data integrity while ensuring efficient system performance.

3.1 User Identity Registration

The identity registration process begins when a user's personal information is entered into the system. This data may include attributes such as user ID, name, age, department, academic year, and photo reference. The collected information is stored in a secure MongoDB Atlas database.

To ensure data integrity, a deterministic hash of the user identity record is generated using the SHA-256 hashing algorithm. The hash is computed using a fixed concatenation format to maintain consistency.

The hash generation process can be represented as:

$$H=SHA256(ID:Name:Age:Branch:Year:PhotoURL)$$

where H represents the identity hash stored on the blockchain.

The generated hash is then submitted to a smart contract deployed on the Ethereum Sepolia blockchain, which stores the hash permanently as an immutable record.

3.2 Authentication and Login

Users authenticate themselves through the mobile application developed using Flutter. The login process includes credential verification using bcrypt password hashing and optional biometric authentication such as fingerprint scanning.

Once the credentials are validated, the application loads the user dashboard and displays the available identity information stored in the database.

3.3 Dynamic QR Code Generation

To enable secure identity verification, the system generates a dynamic QR code that contains the following parameters:

- User ID
- Current timestamp
- Dynamic verification hash

The dynamic verification hash is generated by combining the base identity hash with a timestamp value.

$$Hd=SHA256(Hbase:Timestamp)$$

This dynamic hash ensures that each QR code remains valid only for a limited time interval (30 seconds), preventing attackers from reusing previously captured authentication tokens.

3.4 Verification Process

When a verifier scans the QR code, the system performs the following operations:

1. Extract the user ID and timestamp from the QR code.
2. Retrieve the user identity record from MongoDB.
3. Recalculate the deterministic identity hash.
4. Query the Ethereum Sepolia blockchain to retrieve the stored hash.
5. Compare the recalculated hash with the blockchain hash.

If both values match, the system confirms that the identity record has not been tampered with.

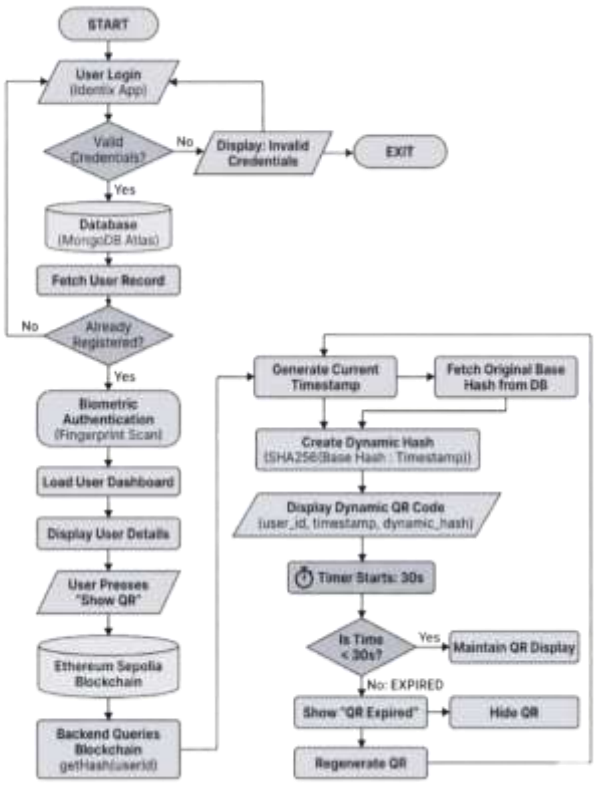

Fig 1. Workflow of the Proposed IDentix Identity Verification System

This verification process ensures that the blockchain acts as an immutable integrity layer for identity validation.

IV. SYSTEM ARCHITECTURE

The proposed IDentix system is designed using a multi-layer architecture that separates the presentation, application, data, and trust layers. This modular architecture improves scalability, security, and maintainability.

A. Presentation Layer

The presentation layer consists of the Flutter mobile application that provides the user interface for both identity holders and verifiers. The user module includes biometric authentication, profile viewing, and dynamic QR code generation. The verifier module includes QR scanning functionality and displays verification results.

B. Application Layer

The application layer is implemented using a Node.js and Express.js backend server. This layer handles authentication, API requests, hashing operations, and blockchain interactions.

The application layer includes three main services:

- Authentication Service – Handles user login, password hashing, and session management using JWT tokens.
- Hashing Engine – Generates deterministic identity hashes and dynamic verification hashes using SHA-256.
- Blockchain Adapter – Communicates with Ethereum smart contracts using Web3.js or Ethers.js libraries.

C. Data Layer

The data layer uses MongoDB Atlas, a cloud-based NoSQL database that stores user identity information, hashed passwords, and verification metadata.

This layer ensures fast data retrieval and supports scalable storage for large numbers of identity records.

D. Trust Layer

The trust layer consists of the Ethereum Sepolia blockchain network, where a smart contract maintains mappings between user identifiers and their corresponding identity hashes.

Because blockchain records are immutable, any unauthorized modification to the stored identity data can be easily detected during verification.

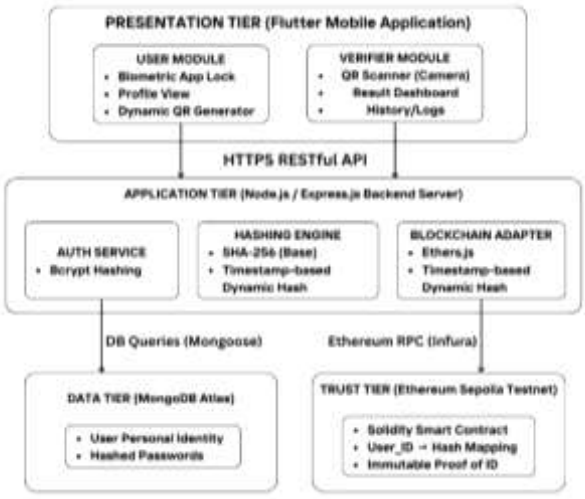

Fig 2. System architecture of the proposed IDentix platform.

V. IMPLEMENTATION AND EVALUATION

The IDentix system was implemented using a combination of modern software development frameworks and blockchain technologies.

The mobile application was developed using Flutter, which provides cross-platform compatibility for Android devices. The backend services were implemented using Node.js and Express.js, while MongoDB Atlas was used for cloud-based data storage.

Smart contracts were written in Solidity and deployed on the Ethereum Sepolia test network using development frameworks such as Hardhat.

A. Dataset

To evaluate the system, a dataset containing more than 200 institutional student identity records was imported into MongoDB. Each record included attributes such as student ID, name, age, academic branch, graduation year, and photo reference.

B. System Performance

The implemented system demonstrated the following performance characteristics:

- Successful blockchain hash storage for all user records
- Real-time QR verification functionality
- Consistent identity hash regeneration
- Accurate detection of tampered records

The dynamic QR authentication mechanism effectively prevented replay attacks by ensuring that authentication tokens expired after 30 seconds.

C. *Security Evaluation*

The proposed system improves security in multiple ways:

- Blockchain immutability prevents unauthorized modification of identity hashes.
- Cryptographic hashing ensures data integrity.
- Dynamic QR authentication mitigates replay attacks.
- Role-based access control restricts system operations to authorized users.
- Screenshot prevention mechanism.

The evaluation results confirm that integrating blockchain with dynamic authentication mechanisms significantly enhances identity verification security.

Table I below compares key features of IDentix to traditional and federated identity approaches. IDentix's decentralized trust model and user-centric control stand in contrast to centralized systems:

Table I. Comparison of identity verification approaches.

Approach	**Trust Model**	**User Control**	**Data Storage**
Centralized IAM	Central authority^[a]	Low	Central server
Federated SSO	Central authority + SSO^[b]	Medium	Central server
IDentix (Proposed)	Decentralized blockchain network	High	Distributed ledger

^a Single organization (e.g. government DB) controls identities.
^b SSO: Single Sign-On across services via identity provider.

Overall, our implementation demonstrates that a two-column blockchain identity framework is practical. It combines cryptography and consensus to achieve the security goals identified in prior work, while using standard blockchain infrastructure (Ethereum Sepolia) for deployment.

VI. RESULTS AND DISCUSSION

The performance of the proposed IDentix system was evaluated based on its ability to ensure data integrity, prevent unauthorized access, and provide real-time identity verification. The evaluation was conducted using a dataset of more than 200 student identity records stored in MongoDB Atlas and corresponding hash values stored on the Ethereum Sepolia blockchain.

6.1 Data Integrity Verification

The primary objective of the system is to detect unauthorized modifications in identity records. During testing, selected user records were deliberately altered to evaluate the tamper detection capability of the system. The recalculated SHA-256 hash was compared with the hash stored on the blockchain.

The system successfully identified all modified records, as any change in user data resulted in a mismatch between the generated hash and the blockchain-stored hash. This confirms that cryptographic hashing combined with blockchain immutability provides strong guarantees for data integrity, as also demonstrated in previous blockchain-based identity systems [1], [3].

6.2 Dynamic QR Authentication Performance

The dynamic QR authentication mechanism was tested to evaluate its resistance against replay attacks. Each QR code contained a timestamp and a dynamically generated hash, making it valid only for a limited duration of 30 seconds.

Expired QR codes were intentionally reused during testing. The system correctly rejected all expired authentication attempts, displaying a "QR Expired" response. This behavior aligns with security practices in time-based authentication systems, where dynamic tokens prevent credential reuse [5].

The results confirm that integrating time-dependent hashing with QR authentication significantly enhances system security.

6.3 Verification Efficiency

The system was evaluated for real-time performance during identity verification. The verification process includes:

- Fetching user data from MongoDB.
- Regenerating the identity hash.
- Retrieving the hash from the blockchain.
- Performing hash comparison.

Despite involving both off-chain and on-chain components, the system achieved near real-time verification. This demonstrates that hybrid architectures combining traditional databases with blockchain can

maintain performance efficiency while ensuring security, as discussed in [4].

6.4 System Reliability

The system was tested under multiple scenarios, including valid authentication, invalid login attempts, tampered data, and expired QR codes. The results showed that:

- Invalid credentials were consistently rejected.
- Tampered identity data were detected.
- Expired QR codes were invalidated.
- Valid users were authenticated successfully.

These outcomes demonstrate that the system is reliable and behaves predictably under different operational conditions. Similar reliability has been observed in decentralized identity frameworks that utilize blockchain verification mechanisms [2].

6.5 Security Improvements

The proposed system significantly improves security compared to traditional identity verification approaches. Blockchain-based identity systems eliminate single points of failure and provide transparent verification mechanisms [1].

The improvements are summarized in Table I.

Table I

Security Comparison Between Traditional and Proposed System

Security Aspect	Traditional System	Proposed System
Data Integrity	Vulnerable to modification	Protected via blockchain hashing
Replay Attacks	Possible	Prevented using dynamic QR
Trust Model	Centralized	Decentralized validation
Verification Transparency	Limited	Fully auditable

These findings are consistent with prior studies showing that blockchain-based identity solutions improve trust, transparency, and resistance to attacks [3], [5].

6.6 Summary of Results

The experimental evaluation confirms that the IDentix system:

- Accurately detects tampered identity records.
- Prevents replay attacks through dynamic QR authentication.
- Provides efficient real-time verification.
- Enhances overall system security and transparency.

The results demonstrate that integrating blockchain with dynamic authentication mechanisms creates a robust and scalable identity verification system.

VII. CONCLUSION

This paper presented IDentix, a blockchain-based decentralized identity verification system designed to enhance the security and transparency of institutional identity management systems. The proposed architecture integrates blockchain technology, cloud databases, and dynamic QR authentication to create a robust verification framework.

By storing cryptographic hashes of identity records on the Ethereum Sepolia blockchain, the system ensures that identity data cannot be modified without detection. At the same time, storing detailed records in MongoDB maintains system efficiency and scalability.

The implementation results demonstrate that the proposed system can successfully detect tampered identity records while enabling real-time verification through dynamic QR codes. This hybrid approach combines the strengths of traditional databases and blockchain technology.

Future work will focus on integrating decentralized storage systems such as IPFS, implementing zero-knowledge proofs for privacy-preserving verification, and deploying the system on scalable blockchain networks such as Polygon.

VIII. REFERENCES

[1] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," IEEE Security and Privacy Workshops, 2015.

[2] A. Tobin and D. Reed, "The Inevitable Rise of Self-Sovereign Identity," The Sovrin Foundation, 2017.

[3] V. Thadari and G. Kumar, "Blockchain-Based Identity Verification to Mitigate Identity Theft in Digital Banking," International Journal of Research in Modern Engineering and Emerging Technology, vol. 13, no. 7, pp. 49–54, 2023.

[4] Z. Li, Y. Zhang, and H. Jin, "DisIMS: A Distributed Identity Management System via Blockchain," IEEE

Transactions on Dependable and Secure Computing, 2025.

[5] D. Salah, S. Mnasri, and H. Idoudi, "Self-Sovereign Digital Identity in Blockchain-Based Systems for E-Health Cards Management," Procedia Computer Science, vol. 270, pp. 985–993, 2025.