

# A decentralized privacy-preserving and scalable blockchain-based identity management system

Prosper Onagie Yusuf <sup>1</sup>, Abdullahi Mai-Auduga <sup>1</sup>, Samuel Omokhafa Yusuf <sup>2,\*</sup>, Emmanuel Joshua <sup>3</sup> and Caleb Eshikpemi Yusuf <sup>4</sup>

<sup>1</sup> Department of Cyber Security, Air Force Institute of Technology, Kaduna State, Nigeria.

<sup>2</sup> Independent Researcher, Massachusetts, USA.

<sup>3</sup> Independent Researcher, Texas, USA.

<sup>4</sup> Department of Computer Science & IT, Federal University Dutsinma, Katsina State, Nigeria.

International Journal of Science and Research Archive, 2025, 14(02), 511-526

Publication history: Received on 27 December 2024; revised on 02 February 2025; accepted on 05 February 2025

Article DOI: <https://doi.org/10.30574/ijrsra.2025.14.2.0368>

## Abstract

This project proposes a decentralized Identity Management System (IMS) built on blockchain technology, prioritizing user privacy and security. The system enables individuals to create, manage, and share their digital identities securely, leveraging blockchain's immutability and transparency. By utilizing smart contracts, the IMS ensures identity verification and authentication while maintaining user control and consent. This innovative approach addresses current identity management challenges, promoting a secure and decentralized digital identity ecosystem. The project's outcome has far-reaching implications for various sectors where identity management is critical.

**Keywords:** Blockchain technology; Smart Contract; Identity Management System; Ecosystem

## 1. Introduction

In today's digital era, the way people and organizations interact and conduct transactions has been transformed. A fundamental element of these interactions is identity management, which involves verifying and authenticating individuals' identities. Traditional identity management systems, often centralized, encounter significant challenges, such as security vulnerabilities, privacy concerns, and scalability issues. The frequent occurrence of cyber-attacks and data breaches has exposed the weaknesses of these systems, highlighting the urgent need for more robust and secure identity management solutions. This context underscores the importance of developing a decentralized, privacy-preserving, and scalable blockchain-based identity management system.

Traditional identity management systems generally follow a centralized model where a single entity, such as a government agency or a corporation, maintains and controls individuals' identity information. These systems rely heavily on trusted third parties to authenticate and authorize users, making them vulnerable to several inherent risks and limitations. Centralized systems are prime targets for cyber-attacks because compromising a single point of failure can expose the personal information of millions of users. For example, the Equifax data breach in 2017 affected approximately 147 million people, and the 2020 SolarWinds hack infiltrated multiple US federal agencies and numerous private companies (Volz and MacMillan, 2021).

Besides security vulnerabilities, centralized identity management systems also raise significant privacy concerns. Users are often required to disclose extensive personal information to multiple entities, increasing the risk of data misuse and unauthorized access. Additionally, these systems can lead to privacy erosion, as users have little control over how their

\* Corresponding author: Samuel Omokhafa Yusuf.

data is collected, stored, and shared. The rise of data protection regulations, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States, reflects growing concerns over privacy and the need for stricter data protection measures.

Blockchain technology has emerged as a promising solution to the challenges faced by traditional identity management systems. A blockchain is a decentralized ledger that records transactions across a network of computers in a secure, transparent, and immutable manner. This decentralized nature eliminates the need for a central authority, distributing trust across the network and enhancing security. The cryptographic principles underlying blockchain technology ensure that once data is recorded, it cannot be altered without consensus from the network participants, thus providing a high level of data integrity (Santos and Ren 2022).

Blockchain's potential to revolutionize identity management lies in its ability to provide decentralized identity (DID) solutions. DIDs enable individuals to control their own identity information and share it securely without relying on a central authority. By leveraging cryptographic techniques and smart contracts, blockchain-based identity management systems can offer enhanced security, privacy, and user control. This approach aligns with the concept of self-sovereign identity (SSI), where individuals own and manage their identity credentials, deciding when, where, and with whom to share their information (Nguyen et al. 2022)

### 1.1. Problem Statement

Traditional identity management systems, being centralized, face significant challenges such as security vulnerabilities, privacy concerns, and limited scalability, making them increasingly inadequate in the digital age. These systems are highly susceptible to cyber-attacks and data breaches, compromising personal information and providing minimal user control over sensitive data. Blockchain technology, with its decentralized and immutable nature, offers a promising alternative, enhancing security and user autonomy. However, blockchain-based systems introduce their own set of challenges, particularly in ensuring privacy on transparent ledgers, achieving scalability, and addressing the lack of interoperability and cross-compatibility between different blockchain platforms and external systems.

The aim of this project is to design and develop a blockchain-based Identity Management System (IMS) that provides a secure, decentralized, user-centric, and interoperable approach to managing digital identities.

---

## 2. Literature Review

### 2.1. Overview of Blockchain Technology

Blockchain technology, a distributed digital ledger, has revolutionized trade, business, and various industries by eliminating the need for a centralized authority to manage and store data. Blockchain is a chain of time-stamped, immutable data blocks, each controlled by a network of interconnected computers (nodes) and secured through cryptographic techniques. This decentralized system is pseudo-anonymous and has transformed areas such as identification, ownership, and finance (Nakamoto, 2021). Although popularized by Bitcoin in 2008, blockchain concepts, such as David Chaum's "blind signatures," date back to the 1980s. The timestamping of documents, introduced by researchers in 1991, and Hal Finney's Reusable Proof of Work (RPoW) in 2004 were foundational elements that paved the way for blockchain's eventual widespread application (Merkle, 1988).

#### 2.1.1. Core Principles of Blockchain Technology

Blockchain operates on principles that distinguish it from traditional centralized systems, including decentralization, immutability, transparency, and security.

- **Decentralization:** In blockchain, control and decision-making are distributed among nodes, preventing any single entity from controlling the entire network. This peer-to-peer (P2P) approach, where nodes independently verify and validate transactions, reduces the risk of manipulation and single points of failure. Decentralization promotes transparency and fault tolerance, ensuring network continuity even if some nodes fail (Buterin, 2014).
- **Immutability:** Blockchain's immutability ensures that once data is recorded, it cannot be altered. This integrity is achieved through cryptographic hash functions that produce a unique hash for each block, making tampering detectable. Each block also links to the previous block's hash, forming a chain resistant to modifications. Immutability is essential for applications in finance, supply chains, and identity verification, providing a reliable audit trail (Merkle, 1988).

- **Transparency:** Blockchain transparency enables all participants to view recorded transactions, fostering trust and accountability. Public blockchains like Bitcoin and Ethereum make transaction histories visible, though user identities are pseudonymous. This openness aids regulatory compliance and auditing, making blockchain appealing for industries requiring transparency (Buterin, 2014).
- **Security:** Blockchain's security combines cryptographic techniques, consensus mechanisms, and decentralized design to guard against attacks, fraud, and unauthorized access. This multi-layered approach ensures transaction reliability and protects network integrity (Garay et al., 2015).

### 2.1.2. Blockchain Consensus Mechanisms

Consensus mechanisms allow decentralized blockchain networks to reach agreement on the ledger's state. Different algorithms meet various needs, including security, scalability, and energy efficiency:

**Proof of Work (PoW):** PoW requires miners to solve complex puzzles to validate transactions, ensuring network integrity. This resource-intensive process prevents double-spending but consumes significant energy, raising environmental concerns. Once a miner solves a puzzle, the new block is verified and added to the chain, making it tamper-resistant. However, PoW's high energy demand limits its scalability (Narayanan et al., 2016).

**Proof of Stake (PoS):** PoS is an alternative to PoW, selecting validators based on the number of tokens they hold. This approach reduces energy use and increases scalability by eliminating the need for computationally intensive puzzles. PoS encourages validator honesty, as staked assets can be forfeited for malicious behavior. Yet, it is prone to 'nothing at stake' attacks, which PoS systems counter through penalties like slashing (King & Nadal, 2012).

### 2.1.3. Decentralized Identity (DID)

Decentralized Identity (DID) is a framework that allows individuals to control their digital identities independently of centralized systems, addressing security, privacy, and inefficiencies in traditional identity management (Sovrin, 2020). Using blockchain and cryptography, DID systems distribute identity data across a network rather than storing it centrally, which enhances privacy and resilience (uPort, 2018). Central to DID is the concept of Decentralized Identifiers (DIDs), unique, user-controlled IDs tied to cryptographic keys for secure verification. These DIDs are linked to DID Documents, which contain public keys and Verifiable Credentials (VCs) like diplomas or licenses, providing a trusted and cryptographically signed form of verification (W3C, 2022).

The benefits of DID systems extend to both users and organizations. Individuals gain greater control over their information, reducing identity theft risks, while organizations can simplify verification processes, reduce compliance costs, and foster trust with users (Akbar et al., 2021). DID systems also use Zero-Knowledge Proofs (ZKPs), allowing users to confirm attributes (e.g., age) without disclosing sensitive details (Zhang et al., 2020).

VCs enhance trust by preventing forgery through cryptographic verification (W3C, 2022). Overall, DIDs improve user control, privacy, security, and interoperability, supporting a more user-centric, flexible identity framework that transcends platform limitations (W3C, 2023).

### 2.1.4. Self-Sovereign Identity (SSI)

Self-Sovereign Identity (SSI) builds on the concept of Decentralized Identifiers (DIDs) to allow individuals to own, manage, and share their identity data securely and privately. This approach enables selective disclosure, meaning individuals can choose which aspects of their identity to share in specific contexts. SSI aims to give users control over their data, regardless of whether it was issued by a government, company, or organization, ensuring a high level of granularity in determining who has access to specific pieces of information (Der et al., n.d.).

SSI is a new online identity management paradigm where individuals and entities store identity information locally or on a distributed network. This allows users to grant access to their data without needing intermediaries, fostering greater control over personal information. Digital identifiers come in various formats, and standardization is necessary for global interoperability (Mühle et al., 2018).

## 2.2. Privacy-Preserving Mechanisms in Decentralized Identity Management Systems (DIMS)

Decentralized Identity Management Systems (DIMS) present a transformative approach to user control and data ownership compared to traditional centralized systems. By removing the reliance on single entities, DIMS enhance security and empower users. However, ensuring robust privacy measures remains a significant challenge. Several privacy-preserving mechanisms have been developed to address this issue.

### *2.2.1. Decentralized Storage and Access Control*

At the core of DIMS is decentralized storage, where data is distributed across multiple nodes rather than residing on a single server controlled by a central authority. This approach mitigates single points of failure and enhances data security. Distributed Ledger Technology (DLT), such as blockchains, underpins many DIMS by securely storing identity data, making unauthorized access challenging (Chen et al., 2019). Moreover, Access Control Mechanisms allow users to define access policies within Decentralized Identifiers (DIDs), specifying who can access their data and under what circumstances (W3C, 2022).

### *2.2.2. Advanced Cryptographic Techniques*

Privacy in DIMS is further strengthened through cryptographic innovations. Zero-Knowledge Proofs (ZKPs) enable users to prove possession of certain attributes without revealing sensitive information, thereby limiting unnecessary data exposure (Zhang et al., 2020). Users can selectively disclose attributes from Verifiable Credentials (VCs), enhancing transactional privacy.

### *2.2.3. Pseudonymity and Ring Signatures*

To protect user anonymity, pseudonymity allows users to interact with systems using pseudonyms rather than real identities, reducing the exposure of personally identifiable information (PII). Similarly, Ring Signatures verify a user's membership in a group without revealing their identity, safeguarding anonymity in group-based proofs.

### *2.2.4. Homomorphic Encryption*

Lastly, Homomorphic Encryption enables computations on encrypted data without decryption, allowing secure data analysis. While promising, its computational demands currently limit widespread adoption in DIMS due to scalability concerns.

These privacy-preserving mechanisms illustrate the innovative strides in protecting user data within DIMS, though challenges remain in achieving broad adoption and operational efficiency.

## **2.3. Scalability Solutions in Blockchain-based DIMS**

To address scalability challenges in blockchain-based Decentralized Identity Management Systems (DIMS), Layer 2 solutions play a critical role by processing transactions off-chain while ensuring the main chain's security.

One such approach is sharding, which divides the blockchain into smaller segments called shards. Each shard processes transactions independently, significantly boosting network throughput (Dang, Dinh, & Chang, 2019). Sidechains offer another solution by operating as separate blockchains parallel to the main chain, facilitating the transfer of data and assets while alleviating the main chain's transaction burden (Back et al., 2014). Additionally, state channels enable transactions to occur off-chain between participants. These channels only update the blockchain when closed, thus reducing congestion and enhancing transaction speed (Buterin, 2022).

These Layer 2 mechanisms collectively enhance the scalability of blockchain systems, making them more efficient and viable for widespread adoption in decentralized identity management.

## **2.4. Challenges and mitigation Strategies in DIMS**

Decentralized Identity Management Systems (DIMS) face several challenges, including security threats, interoperability issues, and user adoption barriers, requiring targeted mitigation strategies.

Security Threats such as Sybil attacks, where multiple fake identities are created to manipulate networks, can be mitigated through robust identity verification and consensus algorithms like proof-of-work or proof-of-stake (Douceur, 2002). Phishing and social engineering exploits human vulnerabilities; countermeasures include user education and multi-factor authentication (Jakobsson & Myers, 2006). Additionally, smart contract vulnerabilities can be exploited if not adequately secured. Regular audits, formal verification, and secure coding practices help prevent such attacks (Atzei, Bartoletti, & Cimoli, 2017).

Interoperability Issues, especially cross-chain communication, challenge seamless data exchange across blockchain networks. Solutions like atomic swaps and interoperability protocols such as Polkadot and Cosmos address these issues (W3C, 2023).

Finally, User Adoption Barriers, stemming from limited understanding and trust, can be addressed by user education and creating intuitive, user-friendly interfaces (Kuperberg, 2023).

## 2.5. Review of Related Works

Several research related to the topic were reviewed and presented in Table 1.

**Table 1** The review of related works

Author	Title of Literature and Year	Key Findings	Methodology	Research Gap
Aarti et al.,	"Blockchain aware decentralized identity management and access control system" (2024)	Proposed a blockchain-based decentralized identity management and access control system that allows users to control their identities.	Design and implementation	It does not provide a thorough evaluation of the proposed system's performance, scalability, and real-world applicability.
James Howell	"Decentralized Identity Challenges and Solutions" (2023)	The article outlines the challenges of decentralized identity systems, such as scalability, interoperability, and user adoption	The article uses case studies and technological analysis, such as the Microsoft ION project, to explain the limitations	The research gap lies in the lack of standardization and seamless cross-platform integration.
J.W. Bambacht, J.A. Pouwelse	"Web3: A Decentralized Societal Infrastructure for Identity, Trust, Money, and Data" (2022)	Proposed a decentralized identity management system that allows users to control their identities and interact with service providers directly.	Design science research	The paper lacks a deeper technical analysis of the practical challenges and considerations in deploying self-sovereign identity solutions.
Tripti Rathee, Parvinder Singh	"A systematic literature mapping on secure identity management using blockchain technology" (2021)	Blockchain technology can address most of the identity management challenges. Proof of Work is the most popular consensus mechanism.	Systematic literature mapping	It lacks a detailed discussion on the specific design principles, architectures, and evaluation criteria for self-sovereign identity systems.
Shuaib et al.,	"Self-sovereign identity for healthcare using blockchain" (2021)	Blockchain-based self-sovereign identity solution can solve patient information privacy and security threats in healthcare.	Literature review	It lacks a broader discussion on the general requirements and challenges of implementing self-sovereign identity systems beyond the healthcare context
Stockburger et al.,	"Blockchain-Enabled Decentralized Identify Management: The Case of Self-Sovereign Identity in Public Transportation" (2021)	Proposed a blockchain-based decentralized identity management system based on self-sovereign identity principles for public transportation.	Design science research	The paper lacks a detailed technical evaluation of the proposed prototype and the practical challenges that may arise during the implementation and deployment of self-sovereign identity

				systems in diverse use cases.
Fennie Wang, Primavera De Filippi	"Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion" (2020)	Blockchain-based self-sovereign identity can help achieve economic inclusion for migrants and other vulnerable populations by allowing them to establish a persistent identity and credit history.	Literature review	Does not provide a deep technical analysis of designing and implementing a self-sovereign identity system.
Omar Dib, Khalifa Toumi	"Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions" (2020)	Provided a comprehensive overview of decentralized identity systems, including their architecture, components, lifecycle, and challenges. Evaluated existing solutions based on the principles of self-sovereign identity.	Literature review, qualitative analysis	Does not include any quantitative performance studies or evaluations of the discussed decentralized identity systems.
Alan Bachmann et al.,	"Decentralized Identity: Where Did It Come from and Where Is It Going?" (2019)	Provided a historical perspective on the evolution of digital identity models, from centralized to self-sovereign, and discussed the current state and challenges of decentralized identity.	Overview of the field	Need for more standards and interoperability between different decentralized identity solutions.
Geoff Goodell, Tomaso Aste	"A Decentralized Digital Identity Architecture" (2019)	Proposed a decentralized digital identity architecture using distributed ledger technology to promote a competitive marketplace for identity services and protect user privacy.	System design	Missing a thorough technical evaluation of the proposed decentralized identity architecture.
Lundkvist et al.,	"uPort: A Platform for Self-Sovereign Identity" (2016)	uPort is a blockchain-based self-sovereign identity solution that allows users to own and control their identities, credentials, and digital assets. It uses smart contracts, a mobile app, and developer libraries.	System architecture description	Lacks a detailed evaluation of the practical challenges in deploying the uPort decentralized identity solution.

### 3. Material and methods

This section details the methodology for developing a blockchain-based Identity Management System (IMS), designed to leverage blockchain's benefits of decentralization, security, and transparency in order to overcome the limitations of centralized identity systems.

### 3.1. Research and Initial Setup

The research phase involved evaluating various blockchain platforms and development tools to determine the most suitable ones for the IMS. The Ethereum blockchain was chosen for its strong infrastructure and smart contract support, and Next.js was selected for front-end development to create a performant web application. Hardhat, a robust Ethereum development environment, was used to streamline the process of building and testing smart contracts (Santos & Ren, 2022).

### 3.2. Blockchain Selection and Setup

Ethereum was selected as the primary blockchain platform for its extensive adoption and support for decentralized applications. Hardhat facilitated the writing, testing, and deployment of Solidity smart contracts, allowing for an efficient development process. The Privy service was integrated to enhance data encryption and privacy, ensuring that sensitive data remains secure. Chainlist enabled network management across Ethereum environments, supporting the IMS's multi-network functionality.

### 3.3. Smart Contract Development

Smart contracts, the core of the IMS, were developed in Solidity using the Hardhat environment. Key functionalities covered by the smart contracts include:

- **User Registration:** A contract was developed to allow user registration and decentralized identity creation, ensuring each identity is unique.
- **Identity Verification:** This contract enabled verification processes, making identity data immutable and tamper-proof.
- **Identity Management:** Contracts were created to allow users to update and manage their identity information securely.
- **Authentication:** Cryptographic methods were employed to implement a contract-based authentication system, ensuring secure user access.
- **Data Storage:** Pinata, a decentralized storage solution, was used to securely store user data off-chain while maintaining blockchain references for data integrity.

Each contract was rigorously tested with Hardhat's testing suite to ensure security and performance (Nguyen et al., 2022).

### 3.4. IMS Development

For the front-end, Next.js was selected for its scalability and performance in web application development, and Shadcn was used for styling to create a cohesive user interface. The Next.js front-end application was integrated with the Ethereum blockchain, enabling user interactions with deployed smart contracts. Privy was used on the client side to handle sensitive user data securely. Key functions of the front-end include:

- **User Registration Interface:** Allows users to create and register decentralized identities.
- **Identity Verification Interface:** Enables users to verify their identity through the IMS.
- **Data Management:** Integrates with Pinata to manage identity documents, which are securely stored off-chain.

### 3.5. Testing and Debugging

Comprehensive testing was conducted to ensure functionality and security, including:

- **Unit Testing:** Tested individual smart contracts and front-end components.
- **Integration Testing:** Examined interactions between Next.js, Privy encryption, smart contracts, and Pinata.
- **Debugging:** Identified and resolved issues, updating both the smart contracts and front-end for a seamless user experience.

### 3.6. Deployment and Maintenance

After testing, the smart contracts were deployed on the Polygon zkEVM Cardano Testnet using Hardhat. The Next.js application was launched in a production environment for high availability. Pinata hosts off-chain data, ensuring it remains securely accessible. Documentation was provided for user interaction and identity management, with maintenance procedures established to monitor and update the IMS as necessary (Volz & MacMillan, 2021).

## 4. Implementation

This section presents the practical implementation of a decentralized, privacy-preserving, and scalable blockchain-based Identity Management System (IMS) is thoroughly examined. This includes setting up the development environment, coding, testing, deploying the system, and analyzing its performance. The chapter's objective is to show how the methodologies presented in Chapter Three were applied to meet the project's goals, creating a comprehensive framework that could be practically deployed.

### 4.1. Development Environment and Tools

Developing the blockchain-based IMS required a carefully planned and configured environment, as well as a range of specialized tools and frameworks that supported each stage of the development lifecycle. This section describes the primary platforms and tools used, along with their significance in developing the system.

#### 4.1.1. Blockchain Platform: Polygon zkEVM Cardano Testnet

The Polygon zkEVM Cardano Testnet was selected as the blockchain platform due to its compatibility with Ethereum and its Layer 2 capabilities, leveraging zk-rollups to enhance scalability, lower transaction costs, and speed up transaction finality. This choice enabled the system to benefit from the security of the Ethereum network while enhancing transaction throughput and minimizing costs, critical aspects for a scalable Identity Management System.

**Smart Contracts:** The Polygon zkEVM platform supports the deployment of Ethereum-compatible smart contracts. This compatibility allowed us to implement key features of the IMS, such as identity registration, verification, and authentication, using zk-rollups for enhanced performance and security.


**Network Configuration:** The Cardano Testnet was used for testing and deployment, which allowed us to simulate real-world conditions in a secure environment. Chainlist was employed to streamline network management and switching as needed. This configuration ensured that the system functioned effectively under network conditions that would mirror those on the Ethereum mainnet.

#### 4.1.2. Smart Contract Development: Solidity and Hardhat

The system's core logic was developed in Solidity, the high-level programming language designed for Ethereum-compatible networks such as Polygon zkEVM. Hardhat, a development environment tailored for Solidity, was employed to facilitate the writing, testing, debugging, and deployment of smart contracts.

**Hardhat Configuration:** Hardhat offered a suite of tools, including ethers.js for contract interactions and Waffle for testing. This facilitated an efficient workflow, allowing for streamlined testing and optimization of contracts for both gas usage and performance. The following steps outline the initial setup:

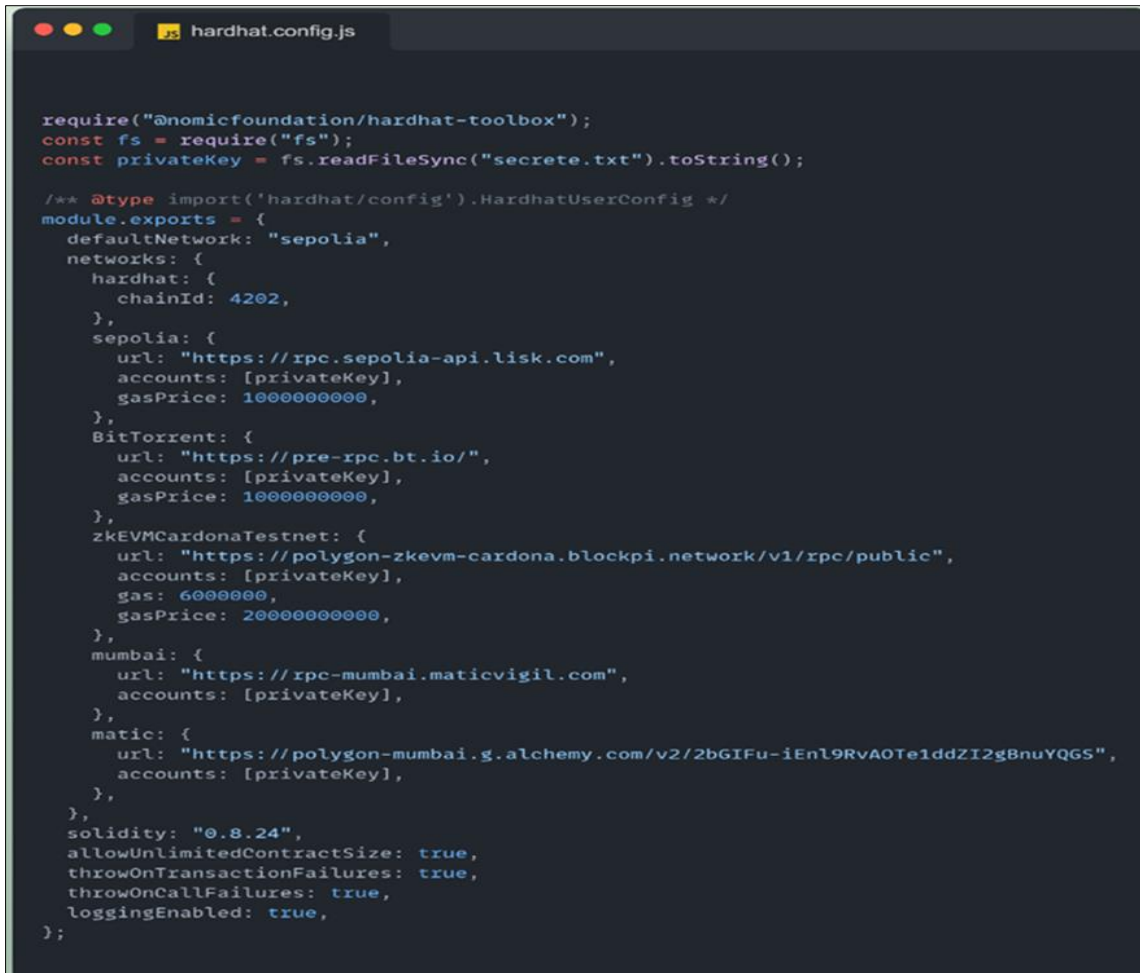
- Step 1: Install Node.js and npm, prerequisites for Hardhat installation.
- Step 2: Navigate to the project directory to specify the installation path for Hardhat.
- Step 3: Install Hardhat as a development dependency.
- Step 4: Modify project files and directories to finalize configuration.



```
npm install --save-dev hardhat
```

**Figure 1** hardhat install

**Hardhat.config.js File:** This configuration file played a crucial role in connecting the project to multiple blockchain networks for testing and deployment.



```

require("@nomicfoundation/hardhat-toolbox");
const fs = require("fs");
const privateKey = fs.readFileSync("secrete.txt").toString();

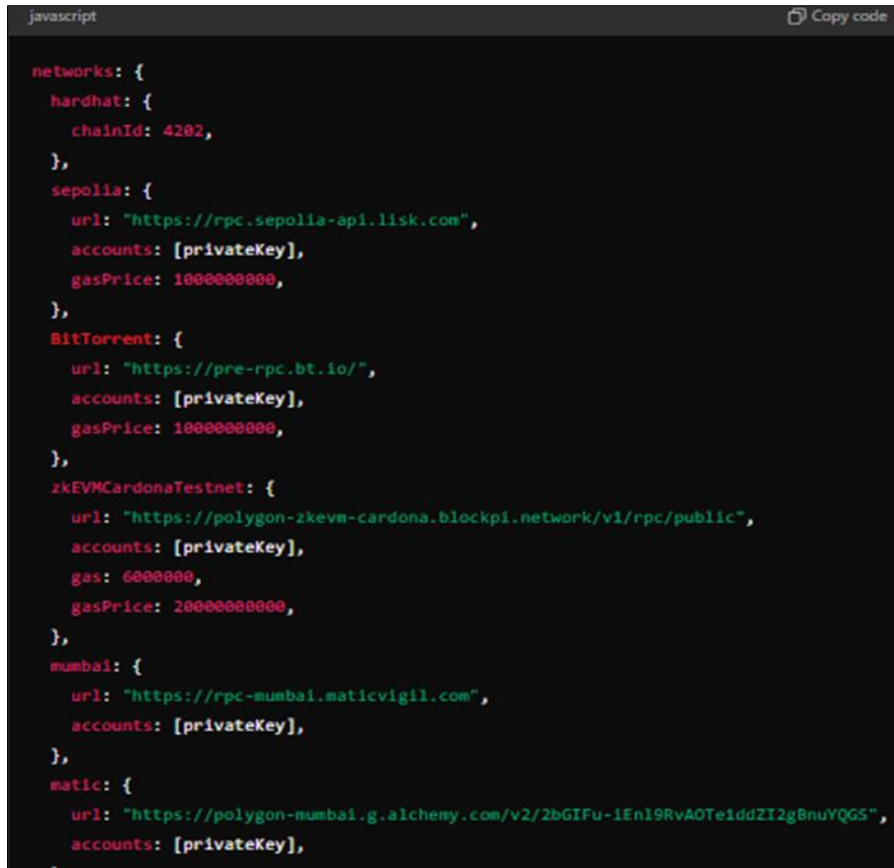
/** @type import('hardhat/config').HardhatUserConfig */
module.exports = {
  defaultNetwork: "sepolia",
  networks: {
    hardhat: {
      chainId: 4202,
    },
    sepolia: {
      url: "https://rpc.sepolia-api.lisk.com",
      accounts: [privateKey],
      gasPrice: 1000000000,
    },
    BitTorrent: {
      url: "https://pre-rpc.bt.io/",
      accounts: [privateKey],
      gasPrice: 1000000000,
    },
    zkEVMCardonaTestnet: {
      url: "https://polygon-zkevm-cardona.blockpi.network/v1/rpc/public",
      accounts: [privateKey],
      gas: 6000000,
      gasPrice: 20000000000,
    },
    mumbai: {
      url: "https://rpc-mumbai.maticvigil.com",
      accounts: [privateKey],
    },
    matic: {
      url: "https://polygon-mumbai.g.alchemy.com/v2/2bGIFu-iEnl9RvA0Te1ddZI2g8nuYQGS",
      accounts: [privateKey],
    },
  },
  solidity: "0.8.24",
  allowUnlimitedContractSize: true,
  throwOnTransactionFailures: true,
  throwOnCallFailures: true,
  loggingEnabled: true,
};

```

**Figure 2** Hardhat.config.js

#### 4.1.3. Below are key aspects of the setup

- **Dependencies:** The package @nomicfoundation/hardhat-toolbox was installed to bundle essential plugins for smart contract development.
- **Private Key Loading:** A private key was securely stored in secrete.txt and accessed through Node.js's file system module, ensuring security while enabling seamless blockchain interactions.
- **Network Configuration:** Multiple networks were configured, such as Sepolia (for Ethereum testing), BitTorrent, and the Polygon zkEVM Cardano Testnet. This multi-network setup allowed comprehensive testing and provided flexibility for different deployment needs.



```

networks: {
  hardhat: {
    chainId: 4202,
  },
  sepolia: {
    url: "https://rpc.sepolia-api.lisk.com",
    accounts: [privateKey],
    gasPrice: 1000000000,
  },
  BitTorrent: {
    url: "https://pre-rpc.bt.io/",
    accounts: [privateKey],
    gasPrice: 1000000000,
  },
  zkEVMCardonaTestnet: {
    url: "https://polygon-zkevm-cardona.blockpi.network/v1/rpc/public",
    accounts: [privateKey],
    gas: 6000000,
    gasPrice: 200000000000,
  },
  mumbai: {
    url: "https://rpc-mumbai.maticvigil.com",
    accounts: [privateKey],
  },
  matic: {
    url: "https://polygon-mumbai.g.alchemy.com/v2/2bGIFu-1En19RvAOte1ddZI2gBnuYQGS",
    accounts: [privateKey],
  },
}

```

**Figure 3** Network configuration

- Hardhat: This offers a local blockchain network with a unique chain ID (4202), ideal for conflict-free testing. Sepolia, an Ethereum testnet, uses an RPC endpoint and private keys for transaction signing, with gas prices set at 1 Gwei.
- BitTorrent: For BitTorrent, the configurations include RPC endpoints and transaction settings like accounts and gas prices. Polygon zkEVM Cardona Testnet and Mumbai testnet use private keys for secure transaction signing, with specific gas limits and prices. The Polygon mainnet is accessed via Alchemy-provided RPC endpoints.
- The Solidity compiler version 0.8.24 introduces enhanced features and security updates.
- Additional options like allowUnlimitedContractSize enable larger contracts, while debugging aids such as throwOnTransactionFailures and loggingEnabled streamline deployment and testing.

#### 4.1.4. Implementation and Functionality of the DynaID.sol Smart Contract

The DynaID.sol contract is a critical component of the Decentralized Identity Management System. This smart contract provides mechanisms for users to create, manage, and retrieve decentralized identities (DIDs) on the blockchain. Below is a detailed breakdown of its functionality:

- Contract Overview: The DynaID contract enables users to establish and control their digital identities in a decentralized manner, promoting data autonomy and security.
- Unique DIDs: Chainlink's Verifiable Random Function (VRF) is used to assign each user a unique DID.
- Profile Management: Users can store personal, professional, and social details and manage their visibility preferences within the system.

#### Key Components:

**Inheritance from VRFConsumerBase:** By inheriting from Chainlink's VRFConsumerBase, the contract can generate unique DIDs using a secure random number function.

- Structs: Modular structs (e.g., User, BasicInfo, SocialLinks) organize user details, supporting efficient data management and scalability.

- **Mappings:** Various mappings (e.g., users, addressToDID) facilitate quick access to user information, linking usernames to profiles and Ethereum addresses to unique DIDs.
- **Modifiers:** Modifiers such as `onlyUniqueUsername` ensure the uniqueness of usernames, preventing duplication.

#### Functions

- **User Creation and Management:** `createUser()` stores user details, while `editUser()` enables profile updates, supporting a dynamic and user-centered identity system.
- **Batch Processing:** The `batchCreateUsers()` function, enabled by the `IBatch` interface, facilitates the creation of multiple profiles in a single transaction, reducing gas costs and enhancing efficiency.
- **Privacy and Visibility:** Functions like `setVisibility()` empower users to control the accessibility of their personal data, aligning with the project's privacy-preserving goals.

#### 4.1.5. Integration of Authentication Using Privy

Authentication in the application was implemented using Privy, a library that facilitates secure user authentication. Privy's integration involved the following components:

- **PrivyProvider Integration:** The `PrivyProvider` component was wrapped around the root layout of the application, ensuring authentication features were accessible throughout the component tree.
- **Configuration Options:** Several settings were customized
- **Application ID:** A unique ID to associate authentication requests with the application.
- **Appearance:** A customized UI with a light theme, accent color, and custom logo, aligning the authentication interface with the application's design.
- **Embedded Wallets:** Enabled wallet creation for new users, simplifying user onboarding for blockchain interactions.
- **Blockchain Integration:** The `zkEVMCardanoTestnet` network was configured as the default chain, allowing secure interactions within the blockchain ecosystem.
- **Authentication Workflow:** Privy facilitated user login, wallet creation, and secure access, offering a streamlined experience that required minimal user input.

#### 4.1.6. Frontend Implementation Overview for the DIMS

The frontend for the IMS was developed using TypeScript with React, structured around a component-based architecture to ensure maintainability and scalability. Key aspects include:

- **Component-Based Architecture:** React components (.tsx files) enabled the creation of modular, reusable UI elements, promoting efficient UI updates and scaling.
- **Routing and Navigation:** React Router handled navigation, managing transitions between authentication pages, user profiles, and dashboards.
- **State Management:** Using context providers and hooks, the frontend managed global states such as user authentication, ensuring seamless access to key data across components.
- **UI and Styling:** CSS and Shadcn UI were used to style the application, providing a consistent, responsive design in line with user experience goals.
- **Data Fetching and Form Handling:** Data fetching was implemented using React hooks, with forms handling input validation and submission, ensuring a smooth and error-free experience.
- **Backend Communication:** The frontend communicated with backend services through API calls to dynamically fetch and update data, integrating the user interface with the underlying smart contracts and authentication mechanisms

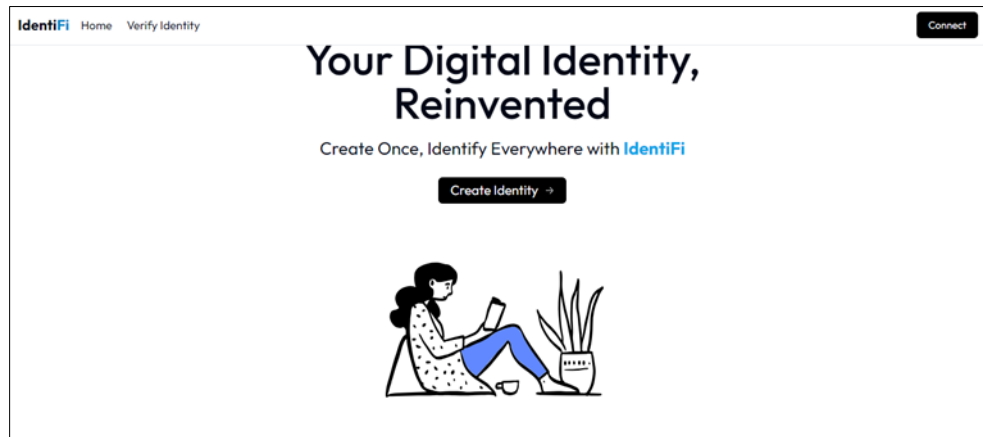
---

## 5. Results and discussion

This section is dedicated to presenting the implementation results within the DIMS (Decentralized Identity Management System) project, specifically focusing on the developed features and functionalities for the blockchain-based Identity Management System. Outlined below are the functionalities and properties of DIMS, which were developed according to the requirements set in the project's objectives. The results demonstrate that the system can efficiently create a Decentralized Identity, Verify the identity and share the identity.

### 5.1. Home Page

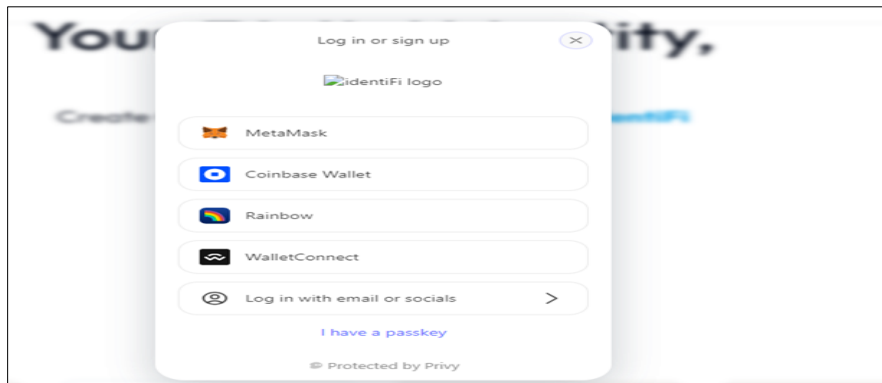
The home page provides an overview of the system, including its features and the services it offers, as depicted in the image below



**Figure 4** DIMS Homepage

### 5.2. Connecting with Wallet

The 'Connect' button on the Decentralized Identity Management System (DIMS) facilitates user authentication by linking a user's blockchain wallet with the platform. When clicked, it triggers a connection process with a wallet provider, such as MetaMask, allowing users to approve and integrate their wallet details with the DIMS. This connection enables secure management of blockchain-based identities and credentials, allowing users to access and interact with their certificates and other features on the platform. The button ensures secure and seamless interaction by leveraging wallet-based authentication to protect user data and maintain system integrity.



**Figure 5** Connect with wallet

### 5.3. Get DID

The 'Get DID' functionality on the DIMS is designed to retrieve and display a user's Decentralized Identifier (DID). When a user interacts with this feature, it triggers a process that queries the blockchain or a decentralized identity service to fetch the DID associated with the user's wallet or account. The DID is a unique, blockchain-based identifier that serves as a secure, verifiable means of representing the user's identity on the platform. This functionality enables users to obtain and view their DID, which is essential for interacting with various decentralized services and verifying their identity within the DIMS ecosystem.

**Creating a DID is a breeze with identiFi**

We making digital identity easier...

**@identiFiDID**

Company GH

identiFi@gmail.com

+00 123 456 789

Skills

UI/UX DevOps

First name \* Satoshi

Last name \* Nakamoto

Username \* satoshinakamoto

Home Address \* 18670 Coastal Highway

Date of Birth \* dd/mm/yyyy

Education \* Harvard

Work History \* Apple, Google, Amazon

Email \* satoshinakamoto@gmail.com

Phone number \* +123456789-0

Figure 6 Get DID

#### 5.4. Verify Identity

The 'Verify Identity' functionality on the Decentralized Identity Management System (DIMS) website allows users to confirm their identity by checking their credentials against the blockchain or a decentralized identity network. When a user requests verification, the system ensures that their provided information matches their Decentralized Identifier (DID) and has not been altered. This process confirms the user's identity securely, using blockchain technology to ensure that the verification is accurate and reliable.

**Verify any Identity**

Enter identiFiDID e.g. satoshinakamoto

Verify

Figure 7 Verify identity

## 6. Conclusion

The successful implementation of this project demonstrates the potential of blockchain technology to revolutionize digital identity management. By providing a secure, decentralized, and privacy-preserving system, the DIMS developed addresses many of the shortcomings of traditional identity management solutions. With further research and development, this system could become a cornerstone of secure digital interactions in various sectors, including finance, healthcare, and education.

#### Recommendation

Based on the findings and conclusions, the following are recommended:

- While a functional DIMS was successfully developed; further research is needed to explore additional privacy-preserving techniques and their integration into the system. This includes exploring the potential of homomorphic encryption for more secure data processing and storage.
- Although the system demonstrated scalability, future work should focus on optimizing the scalability solutions, particularly in handling a large number of transactions and users simultaneously. Exploring other Layer 2 solutions or implementing sharding techniques may provide further improvements.
- One of the challenges identified was the user adoption barrier due to the complexity of decentralized systems. Developing comprehensive user education programs to help users understand the benefits and functionalities of the DIMS is recommended. Simplifying the user interface and experience will also aid in wider adoption.
- As identity management systems are subject to various regulations, it's essential to ensure that the DIMS complies with relevant laws and standards, such as GDPR. Future work should include a focus on ensuring that the system meets all necessary regulatory requirements.

- To enhance the utility of the DIMS, it is recommended to explore and implement interoperability with other identity management systems and services. This will allow users to seamlessly integrate their decentralized identities across different platforms and applications.
- Given the critical nature of identity management, conducting regular security audits and updates to the DIMS is recommended. This will ensure that the system remains resilient against emerging threats and vulnerabilities.

#### *Future works*

- As technology continues to evolve, there are several areas where this project could be expanded and improved in the future:
- Future developments could explore the integration of AI and machine learning algorithms to enhance the system's capabilities. For example, AI could be used to detect and prevent fraudulent activities by analyzing patterns in identity verification processes.
- Expanding the DIMS to be compatible with more platforms and devices would greatly increase its accessibility and usability. This could involve developing mobile applications or integrating with existing digital identity platforms.
- As privacy concerns continue to grow, future work could focus on implementing advanced privacy-preserving techniques, such as differential privacy or more sophisticated cryptographic methods, to further protect user data.
- For the DIMS to have a global impact, future research should look into creating standardized protocols that can be adopted internationally. This would involve collaborating with global organizations to set standards for decentralized identity management.
- Continuous improvements to the user interface and experience will be necessary to ensure that the system is intuitive and easy to use. Future work could involve user testing and feedback loops to refine the design and functionality.

---

### **Compliance with ethical standards**

#### *Disclosure of conflict of interest*

No conflict of interest/ Competing Interests in the publication of the manuscript or with any institution or product that is mentioned in the manuscript and/or is important to the outcome of the study presented.

---

### **References**

- [1] Agarkar AA, Karyakarte M, Patil M. Blockchain-aware decentralized identity management and access. ScienceDirect. 2024.
- [2] Agarkar AA, Karyakarte M, Patil M. Blockchain-aware decentralized identity management and access. ScienceDirect. 2024.
- [3] Ahl A, Yarime M, Tanaka K, Sagawa D. Exploring blockchain for the energy transition: Opportunities and integrating this technology with other digital innovations. Renew Sustain Energy Rev. 2020.
- [4] Akbar et al. Decentralized identity. Article for Blockchain. 2021.
- [5] Allen C. The path to self-sovereign identity. J Decentralized Identity Syst. 2022.
- [6] Atzei N, Bartoletti M, Cimoli T. A survey of attacks on Ethereum smart contracts. Int. Conf. Principles of Security and Trust. 2017:164-86.
- [7] Back A, Corallo M, Dashjr L, Friedenbach M, Maxwell G, Miller A, et al. Enabling blockchain innovations with pegged sidechains. arXiv. 2014.
- [8] Bambacht J, Pouwelse J. Web3: A decentralized societal infrastructure for identity, trust, money, and data. Cornell University. 2022.
- [9] Buterin V. A next-generation smart contract and decentralized application platform. Ethereum White Paper. Available from: <https://ethereum.org/en/whitepaper/>
- [10] Buterin V. State Channels: Scaling Solutions for Blockchain. J. Blockchain Technol. 2022.

- [11] Buttar M, Anwar M. Decentralized identity management using blockchain technology: Challenges and solutions. In: Buttar M, editor. 2024 Feb 13. doi:10.1007/978-3-031-49593-9\_8.
- [12] Chen et al. A blockchain-based decentralized identity management system. IEEE Access. 2019
- [13] Dang H, Dinh TT, Chang EC. Sharding blockchain: State of the art and research challenges. arXiv preprint. 2019.
- [14] Der U, Jähnichen S, Sürmeli J. Opportunities and challenges for the digital revolution. Self-sovereign identity: preprint arXiv:1712.01767.
- [15] Douceur JR. The Sybil attack. In: Proc Int Workshop on Peer-to-Peer Syst; 2002. p. 251–60.
- [16] Garay J, Kiayias A, Leonardos N. The Bitcoin Backbone Protocol: Analysis and applications. In: Proc Ann Int Conf Theory Appl Cryptographic Technol; 2015. p. 281–310. Springer, Berlin.
- [17] Howell J. Decentralized identity – Challenges & solutions. 101 Blockchains. 2023.
- [18] Huckle S, White M. Towards a decentralised identity management ecosystem. ScienceDirect. 2022.
- [19] Jakobsson M, Myers S. Phishing and countermeasures: Understanding the increasing problem of electronic identity theft. Wiley Publishing; 2006.
- [20] Javed IT, Alharbi F, Margaria T, Crespi N, Qureshi KN. Health-ID: A blockchain-based decentralized identity. MDPI. 2021.
- [21] King S, Nadal S. Peer-to-peer crypto-currency with proof-of-stake. PPcoin White Paper. 2012. Available from: <https://www.peercoin.net/assets/paper/peercoin-paper.pdf>
- [22] Kuperberg M. Towards self-sovereign identity using blockchain technology. Blockchain Appl. Identity Manag. 2023;11(2):37-50.
- [23] Mühle A, Grüner A, Gayvoronskaya T, Meinel C. A survey on essential components of a self-sovereign identity. ScienceDirect. 2018.
- [24] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Bitcoin. 2021 Mar 14. Available from: <https://bitcoin.org/bitcoin.pdf>
- [25] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Bitcoin White Paper. 2008.
- [26] Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S. Bitcoin and Cryptocurrency Technologies. Princeton University Press; 2016.
- [27] Nguyen K, Zhang Q, Miao. Self-sovereign identity with blockchain for cross-domain authentication. IEEE Trans Inf Forensics Secur. 2022.
- [28] Pease R, Dunphy P, Petitcolas FA. Towards a more secure and private decentralized identity ecosystem. IEEE Access. 2022;10.
- [29] Preukschat A, Reed D. Self-Sovereign Identity. Manning Publications; 2021.
- [30] Rathee T, Singh P. A systematic literature mapping on secure identity management. SystemDirect. 2024.
- [31] Santos J, Ren K. Blockchain for privacy-preserving identity management: Challenges and solutions. IEEE Internet Things J. 2022.
- [32] Sovrin. Decentralized identity: A new paradigm for identity management. Sovrin. 2020.
- [33] Sporny M, Longley D, Chadwick DW. Verifiable Credentials Data Model v1.1. W3C. 2022. Available from: <https://www.w3.org/TR/vc-data-model/>
- [34] Stockburger L, Kokosioulis G, Mukkamala A, Rao R. Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. ScienceDirect. 2021.
- [35] Tobin A, Reed D. The inevitable rise of self-sovereign identity. The Sovrin Foundation. 2017;29.
- [36] uPort. Decentralized identity: A new era for identity management. uPort. 2018
- [37] Volz D, MacMillan R. SolarWinds hack breached Justice Department system. Wall Street Journal. 2021.
- [38] W3C. Decentralized identifiers (DIDs) v1.0. World Wide Web Consortium. 2022 Jul 19. Available from: <https://www.w3.org/TR/did-core>

- [39] W3C. Decentralized identifiers (DIDs). World Wide Web Consortium. 2023. Available from: <https://www.w3.org/TR/did-core/>
- [40] W3C. Verifiable credentials data model 1.0: Expressing verifiable information on the web. World Wide Web Consortium Recommendations. 2023.
- [41] Wang F, De Filippi P. Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion. *Front Blockchain*. 2020.
- [42] Zhang Y, Chen X, Li J, Zhang Z, Sun X. Identity-based attribute-based encryption with short ciphertexts for verifiable credentials. *IEEE Int. Conf. Comput. Sci. Eng. (CSE)*. 2020b;1449-56.
- [43] Zhang Y, Xu X, Chen X, Li J, Sun X. A survey on privacy-preserving techniques for decentralized identity management. *Int. Conf. Security, Privacy, and Pattern Recognition (SECURWARE)*. 2020a;142-7.