# Architecture for self-sovereign management of personal data implementing decentralized networks

## *Arquitectura para la gestión auto soberana de datos personales implementando redes descentralizadas*

## *Arquitetura para a gestão autônoma de dados pessoais por meio da implementação de redes descentralizadas*

**Omar Ricardo Castellanos Hernández**[1]
**Roberto Albeiro Pava-Díaz**[2]

**Received:** December 10th, 2025
**Accepted:** March 16th, 2026
**Available:** May 5th, 2026

**How to cite this article:**
O. R. Castellanos Hernández and R. A. Pava-Díaz, "Architecture for Self-Sovereign Management of Personal Data Implementing Decentralized Networks," *Revista Ingeniería Solidaria,* vol. 22, no. 2, 2026.
doi: https://doi.org/10.16925/2357-6014.2026.02.03

Research article. https://doi.org/10.16925/2357-6014.2026.02.03

[1] Master's Degree Candidate in Information and Communication Sciences, Faculty of Engineering, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.
Email: orcastellanosh@udistrital.edu.co
**ORCID:** https://orcid.org/0009-0008-6434-1433
CvLAC: https://acortar.link/2LBtxp

[2] Ph.D. in Engineering, Faculty of Engineering, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.
Email: rapavad@udistrital.edu.co
**ORCID:** https://orcid.org/0000-0003-0440-892X

## Abstract

*Introduction:* This article is one of the derived products of the research project "Administration Model for Personal Information Management Oriented to the Data Owner", conducted within the Master's in Information and Communication Sciences at Universidad Distrital Francisco José de Caldas in Bogotá, Colombia, during the years 2025–2026.

*Problem:* Current administration and control methods for personal data face vulnerabilities related to integrity, transmission, and third-party use.

*Objective:* The objective of this article is to propose an architecture that enables users to achieve decentralization and sovereignty over their personal data.

*Methodology:* A review of the existing literature was conducted, considering implementations in which technological solutions for information management are proposed or applied.

*Results:* A user-centered proposal is presented in which, after comparing different technologies, blockchain stands out for providing sovereignty over personal data and enabling authorized and restrictive access controls.

*Conclusion:* The proposal shifts centralized data custody from third parties to user sovereignty, replacing current intermediary-dominated management structures.

*Originality:* The proposal challenges centralized data storage paradigms by conferring ownership and operational sovereignty to the users to whom the data belong.

*Limitations:* The model is limited by scope and budget constraints during implementation and depends on the specific use case and the prevailing socio-cultural context.


**Keywords:** personal data; privacy; decentralization; blockchain.


## Resumen

*Introducción:* Este artículo es uno de los productos derivados de la investigación "Modelo de administración para la gestión de información personal orientado al propietario de los datos", desarrollada en la Maestría en Ciencias de la Información y la Comunicación de la Universidad Distrital Francisco José de Caldas en Bogotá, Colombia, durante los años 2025–2026.

*Problema:* La administración y los métodos de control de los datos personales enfrentan actualmente problemas de vulnerabilidad en cuanto a la integridad, transmisión y uso por parte de terceros.

*Objetivo:* El objetivo del presente artículo es proponer una arquitectura que permita al usuario la descentralización y la soberanía de sus datos personales.

*Metodología:* Se realizó una revisión de la literatura existente, teniendo en cuenta implementaciones en las que se proponen o aplican soluciones tecnológicas para la gestión de la información.

*Resultados:* Se presenta una propuesta centrada en el usuario en la cual, tras comparar diferentes tecnologías, blockchain destaca por brindar soberanía sobre los datos personales y otorgar controles de acceso autorizados y restrictivos.

*Conclusión:* La propuesta busca transferir la custodia centralizada de los datos desde terceros de confianza hacia la soberanía del usuario, reemplazando las estructuras de gestión actuales dominadas por intermediarios.

*Originalidad:* Se transforman los paradigmas de almacenamiento centralizado de datos hacia esquemas que otorgan control y soberanía operativa al usuario propietario de sus datos personales.

*Limitaciones:* El modelo presenta limitaciones en alcance y presupuesto durante su implementación, y depende del caso de uso y del entorno social y cultural en el que se aplique.

**Palabras clave:** datos personales; privacidad; descentralización; blockchain.

## Resumo

*Introdução:* Este artigo é um dos produtos derivados do projeto de pesquisa "Modelo de Gestão para Gerenciamento de Informações Pessoais Orientado ao Proprietário dos Dados", desenvolvido no âmbito do Programa de Mestrado em Ciências da Informação e Comunicação da Universidade Distrital Francisco José de Caldas, em Bogotá, Colômbia, durante os anos de 2025 e 2026.

*Problema:* Os métodos de gerenciamento e controle de dados pessoais atualmente enfrentam vulnerabilidades quanto à integridade, transmissão e uso por terceiros.

*Objetivo:* O objetivo deste artigo é propor uma arquitetura que permita aos usuários descentralizar e manter a soberania sobre seus dados pessoais.

*Metodologia:* Foi realizada uma revisão da literatura existente, considerando implementações que propõem ou aplicam soluções tecnológicas para o gerenciamento da informação.

*Resultados:* Apresenta-se uma proposta centrada no usuário na qual, após a comparação de diferentes tecnologias, o blockchain se destaca por proporcionar soberania sobre os dados pessoais e conceder controles de acesso autorizados e restritivos. Conclusão: A proposta busca transferir a custódia centralizada de dados de terceiros confiáveis para a soberania do usuário, substituindo as atuais estruturas de gerenciamento dominadas por intermediários. Originalidade: Transforma paradigmas de armazenamento de dados centralizados em esquemas que concedem controle e soberania operacional ao usuário que detém seus dados pessoais.

*Limitações:* O modelo apresenta limitações de escopo e orçamento durante a implementação e depende do caso de uso e do ambiente sociocultural em que é aplicado.

**Palavras-chave:** dados pessoais; privacidade; descentralização; blockchain.

# 1. INTRODUCTION

With technological progress, new computing paradigms related to the value and use of information have emerged, highlighting its importance in terms of collection and processing. Data have become a valuable asset for organizations, which primarily use them to offer services and products [1], as well as to predict market trends and support strategic decision-making. To this end, multiple data collection methods are employed, ranging from surveys to consumption metadata, such as those obtained through social networks, private companies, or government entities for predictive and statistical purposes [2].

Data processing facilitates the management of services and products, benefiting both companies and users by addressing their demands and needs. However, its excessive and uncontrolled use has also led to negative implications regarding data distribution and storage, giving rise to legal and ethical issues such as information

theft [3], fraud, phishing, data breaches [4], and the sale of databases to malicious third parties [5], among others.

Countries and governments have developed regulations to limit the flow and control of information. For example, the European Union established the General Data Protection Regulation (GDPR) [6], a legal framework that grants citizens rights such as erasure, rectification, and access to personal data stored by entities that process information.

In Colombia, the constitutional law "Habeas Data" [7], similar to the GDPR, entered into force on April 19, 2013. This regulation aims to grant users the authority to validate, update, or delete information held by companies through petitions or claims before private entities and, subsequently, governmental institutions. This law applies to all data banks of financial and commercial organizations. Companies, in turn, are required to inform users about the procedures that may be carried out with their data.

To exercise the rights established under the Habeas Data law, users may request from companies the data currently held and the operations being performed, once per month; if requested more frequently, the entity may charge for a credit history report. Additionally, if a claim is required, the user may approach a credit bureau and carry out the corresponding procedure; the maximum response time is 15 business days. Depending on the response provided, if the requested actions are not fulfilled, the user may resort to governmental oversight mechanisms and submit the case while awaiting resolution [8].

However, these complaint procedures present failures and delays on the part of companies and, combined with the administrative burden, time requirements, and bureaucratic processes, result in an exhausting procedure that may not lead to a favorable outcome for the user. This situation often results in abandonment of the process and a general lack of awareness among the public.

Based on an analysis of current systems and their limitations, the main objective is the decentralization of information and the transfer of control to the legitimate user through mechanisms that can be managed directly, without dependence on third parties. This approach seeks to grant users sovereignty over their data, transforming current operational models and enabling greater efficiency and control in interactions with external actors.

## 1.1. Literature Review

A comprehensive bibliographic review was conducted on current methods and procedures whose architectures and functionalities could contribute to improving personal


e-ISSN 2357-6014 / Vol. 22, no. 2 / may-august 2026 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

data management. From this review, several technologies were identified that may address the problem under study, including differential privacy, anonymization and pseudonymization, Identity and Access Management (IAM), cryptographic methods, federated learning (AI), and blockchain, among others. Following this analysis, an in-depth review of each technology will be carried out, with the aim of highlighting their advantages and limitations in terms of use and implementation.

## Differential privacy

In social networks, in order to maintain privacy at the time of information processing, a process known as differential privacy [9] is used, a method in which the obtained information goes through a framework where random noise is added to the data, modifying information that may compromise the user's identity, allowing functional analysis but without real exposure. This processing method has proven beneficial for companies that implement it, but it also presents some risks associated with the balance between the amount of noise and the real data [10], this may lead to inaccuracy in the results or to the actual exposure of the data depending on the percentage implemented in each case. It also presents performance issues, lack of standardization, and regulation [11].

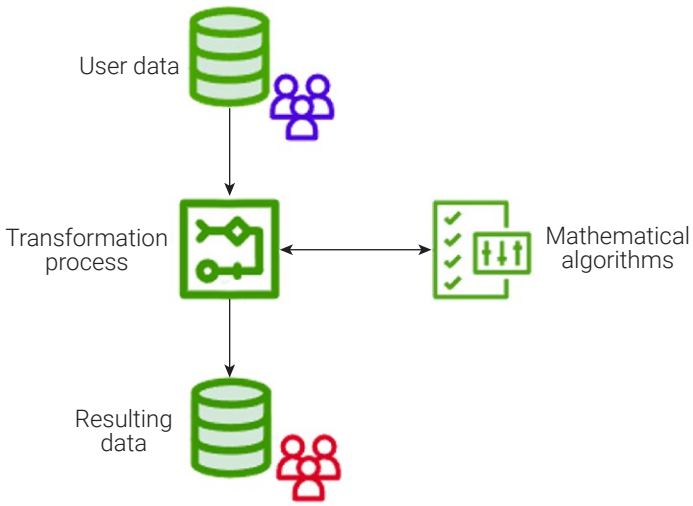


**Figure 1.** Data flow in differential privacy.
**Source:** Own Work

## Anonymization and pseudonymization

A widely used process in the processing of personal data is anonymization and pseudonymization. This procedure, although it shares certain objectives with differential privacy, is based on techniques such as perturbation (adding data that generate noise), suppression of direct identifiers (name, email, phone number), and the treatment of quasi-identifying attributes (age, location, status, disease). Other relevant methods include generalization, which allows grouping specific values into broader categories depending on the use of the information; "k-anonymity," which guarantees that at least k records with the same values must exist; "l-diversity," which ensures the diversity of sensitive values within each group; and finally, "t-closeness," which seeks to keep the distribution of sensitive values as close as possible to that of the overall dataset [12].

This procedure, although more comprehensive, continues to present some flaws; it is possible to identify a person using quasi-identifiers by matching them with other databases or simply by analyzing them. In 2023, through a study, it was demonstrated that, using purchase history information, it is possible to identify an individual with up to 94% probability [13].

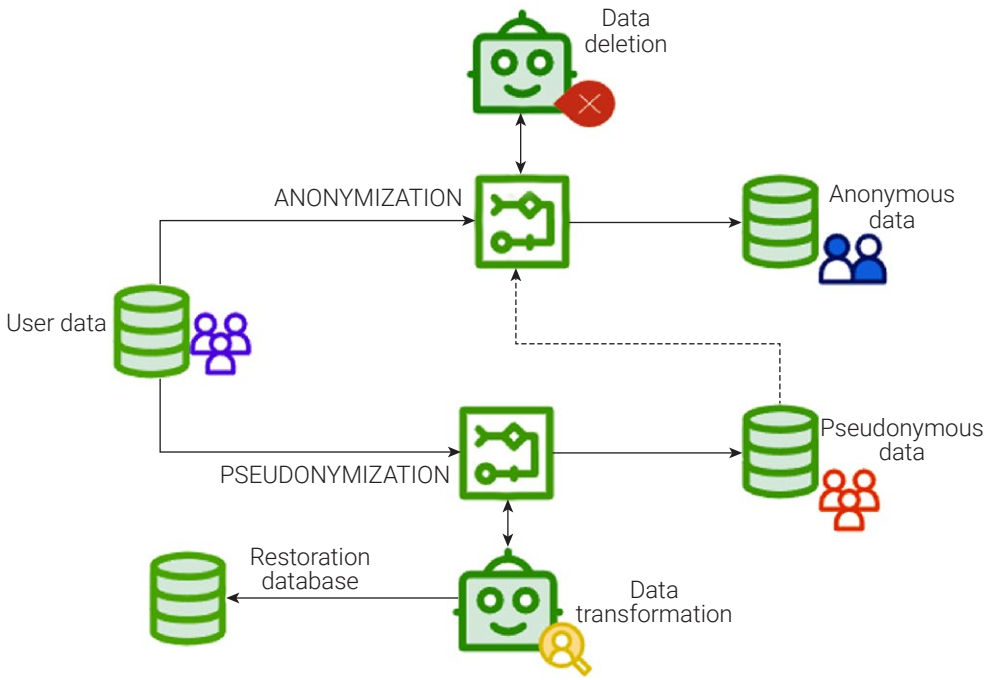


**Figure 2.** Data flow in the Anonymization and Pseudonymization process.
**Source:** Own Work

## Trusted Execution Environments (TEE)

This technology is implemented through an isolated hardware-based environment, which ensures security even from the operating system itself. The system functions as a secure vault and cannot be manipulated by other programs, preventing unauthorized access. To respond to a legitimate information request, the data are received, validated, and processed within this secure environment, always remaining protected and isolated; subsequently, only the required information is exposed [14].

Its main strength lies in its isolation from all software, operating independently and minimizing data exposure. However, this same characteristic represents its primary limitation, as it requires manufacturer-specific hardware and is complex to implement and maintain. Although secure, it is located at a single site, which makes it susceptible to side-channel attacks [15].

## Identity and Access Management (IAM)

IAM access control defines who can use a specific resource within a system and under which conditions. To achieve this, it implements different models, such as RBAC (Role-Based Access Control), which assigns permissions based on user roles; and ABAC (Attribute-Based Access Control), which considers additional parameters such as context or resource ownership to provide greater flexibility. Similarly, the use of federated identity through protocols such as OAuth, OpenID Connect, and SAML enables the use of a single set of credentials across different platforms. Corporate services such as Google, AWS, and Azure are representative examples of these solutions [16]. The main limitation of this approach is that, although robust, it depends on third parties, further centralizing information by relying on a single provider. This dependency can become a vulnerability, representing a single point of failure [17].

## Cryptographic Methods

The application of cryptographic methods incorporates techniques such as homomorphic encryption, which allows operations to be performed on encrypted data without requiring decryption, thereby ensuring confidentiality even during processing. Another relevant mechanism is zero-knowledge proofs (ZKP), which enable the verification of the validity of a statement without directly revealing the underlying data. Additionally, encryption protocols such as TLS and algorithms such as AES represent standard practices in centralized information storage.


e-ISSN 2357-6014 / Vol. 22, no. 2 / may-august 2026 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

Some limitations of this methodology are primarily related to human intervention, including omissions in processes, lack of updates, improper key management, and insufficient infrastructure [18]. Furthermore, certain encryption algorithms have already been compromised by brute-force attacks (e.g., MD5, SHA-1, DES) [19], and others may be vulnerable in the future with the advancement of quantum computing [20].

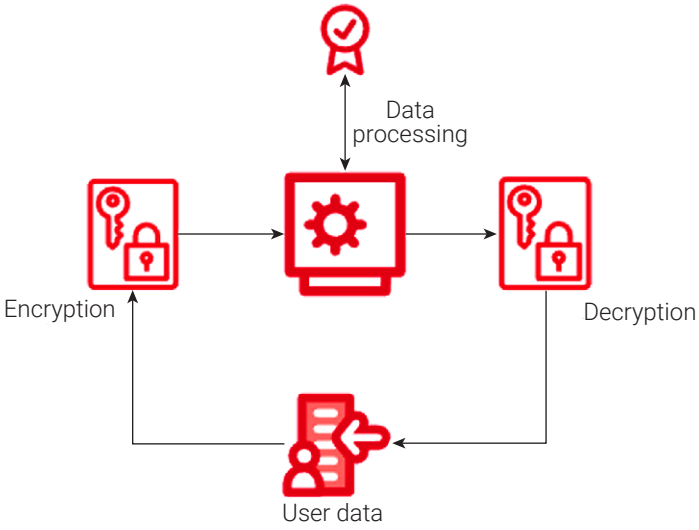


**Figure 3.** Data processing with homomorphic cryptography
**Source:** Own Work

The RSA cryptographic system [21], developed in 1979, is one of the first and most widely used asymmetric encryption algorithms, employing public and private keys. The algorithm relies on the computational complexity of integer factorization, using the product of two large prime numbers. Like other cryptographic methods, its strength increases with advances in computational capacity.

There is also the AES symmetric encryption standard, which operates through a block cipher scheme. Developed in the United States and widely adopted by organizations worldwide [22], AES uses a fixed block size of 128 bits and key sizes of 128, 192, or 256 bits. Documented attacks that have compromised the standard have been limited since the first occurrence in 2005; however, these systems are predominantly applied in centralized data environments under the control of private entities.

## OpenPDS

OpenPDS is a technology that enables users to manage their metadata and limit its exposure to third parties [23]. It operates in conjunction with SafeAnswers [24] and

maintains anonymity by using normalized metadata aggregated from multiple individuals, making it difficult to identify the user initiating a request. OpenPDS implements a secure environment that functions as a centralized repository where user metadata are stored. This technology can be deployed on servers for client consumption or offered through Software as a Service (SaaS) models, allowing users to manage their data and decide which services to access without exposing their identity.

The main drawback of this technology is its centralized nature, which may introduce security vulnerabilities. Additionally, it can impose technical complexity on users due to the lack of standardization.

## Federated Learning in AI

The advancement of artificial intelligence has driven the development of new methods for information processing. One such method is federated learning, in which distributed models are trained on users' devices without centralizing data, transmitting only model update parameters to a central server [25]. This approach is often combined with differential privacy, introducing noise into shared parameters to prevent information inference.

However, this methodology presents several limitations, particularly the risk of reconstruction attacks during information inference [26]. Furthermore, although the system operates in a decentralized manner, malicious participants may send manipulated updates to the server, introducing bias, reducing model accuracy and reliability, or even embedding backdoors into the model [27], [28].

## Blockchain

Blockchain technology is based on a decentralized architecture that operates through a distributed ledger composed of interconnected blocks across a network of nodes, where information is stored in an immutable and verifiable manner [29]. Each transaction is validated through cryptographic hashing and consensus mechanisms among network participants (peer-to-peer), ensuring authenticity, integrity, and traceability without reliance on a central authority. This results in a combination of cryptographic techniques and secure decentralized processes.

In terms of data protection, blockchain addresses the issue differently: rather than storing data directly, it ensures their integrity, management, and controlled exposure to third parties. As the technology continues to evolve, it allows integration with mechanisms such as zero-knowledge proofs (ZKP) [30] and self-sovereign identity

(SSI) [31], granting users greater control over their personal data. Among its limitations, long-term implementation challenges may arise, particularly due to increased computational requirements for operation [32].

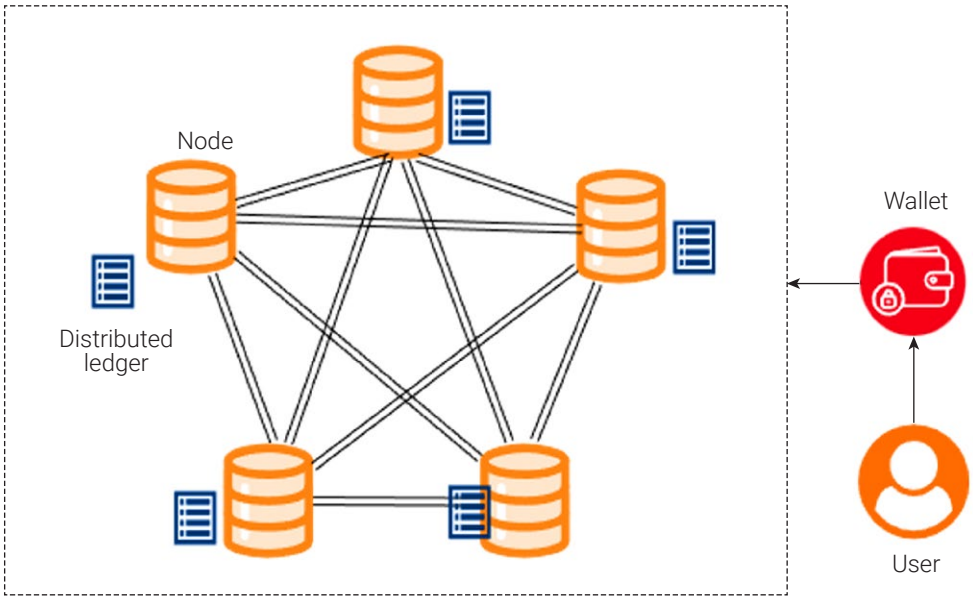


**Figure 4.** Basic blockchain architecture.
**Source:** Own Work

Regarding current technologies, a comparison is carried out among them considering qualities and characteristics that could be implemented in the solution. Factors that impact information storage will be taken into account, such as decentralization, immutability, and resistance to attacks; likewise, the management performed in the process, qualities such as confidentiality, traceability, and overall control, among other properties.

The purpose of the comparison is to obtain the best tool and propose a model based on it that fulfills the objective.

**Table 1.** Comparison among technologies for personal data management

| Characteristics / Technologies | Differential privacy | Anonymization -pseudonymization | TEE | IAM | Cryptographic method. | IA | Blockchain |
|---|---|---|---|---|---|---|---|
| Decentralization | X | X | X | X | X | ✓ | ✓ |
| Individual privacy | ✓ | ✓ | ✓ | X | ✓ | ✓ | ✓ |
| Data integrity | X | X | ✓ | ✓ | ✓ | X | ✓ |
| Information confidentiality | ✓ | X | ✓ | X | ✓ | ✓ | ✓ |
| Transparency and traceability | X | X | X | ✓ | X | X | ✓ |
| Applied anonymity | X | X | X | X | ✓ | X | ✓ |
| Scalability | ✓ | ✓ | X | ✓ | ✓ | ✓ | ✓ |
| Immutable data storage | X | X | X | X | X | X | ✓ |
| Resistance to manipulation | X | X | ✓ | X | ✓ | X | ✓ |
| Access control | X | X | ✓ | ✓ | ✓ | X | ✓ |

**Source:** Own Work

Most technologies offer partial benefits or are focused on specific sectors or areas dependent on third parties; in contrast, blockchain provides the integrity, traceability, and decentralization required for the sovereignty and use of personal data by its owner.

# 2. MATERIALS AND METHODS

Some existing solutions do not fully address users' needs in terms of accessibility, ease of use, and security. Therefore, the development of an architecture is proposed to optimize the processing of personal data, with decentralization, encryption, and security as its core pillars.

Based on the analysis conducted, the main characteristics of existing tools were identified, including dependence on third parties, degree of centralization or decentralization, immutability of information, scalability, and, above all, the difficulty of ensuring traceability and informed user consent. As a result of this analysis, blockchain emerged as one of the most comprehensive models, offering greater advantages compared to other technologies.

For this reason, and considering the analysis performed, blockchain is selected as the base technology, complemented by compatible tools that allow improvements


e-ISSN 2357-6014 / Vol. 22, no. 2 / may-august 2026 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

to its current operation. Among these, advances in the development of self-sovereign identity (SSI) schemes are noteworthy, as well as compatibility with cryptographic security protocols such as zero-knowledge proofs (ZKP), homomorphic encryption, and even post-quantum encryption [33]. This does not necessarily imply the inclusion of all these methods within the design, as some are intended for different purposes, but rather the evaluation and implementation of those that best meet the requirements and fulfill the objectives of this work.

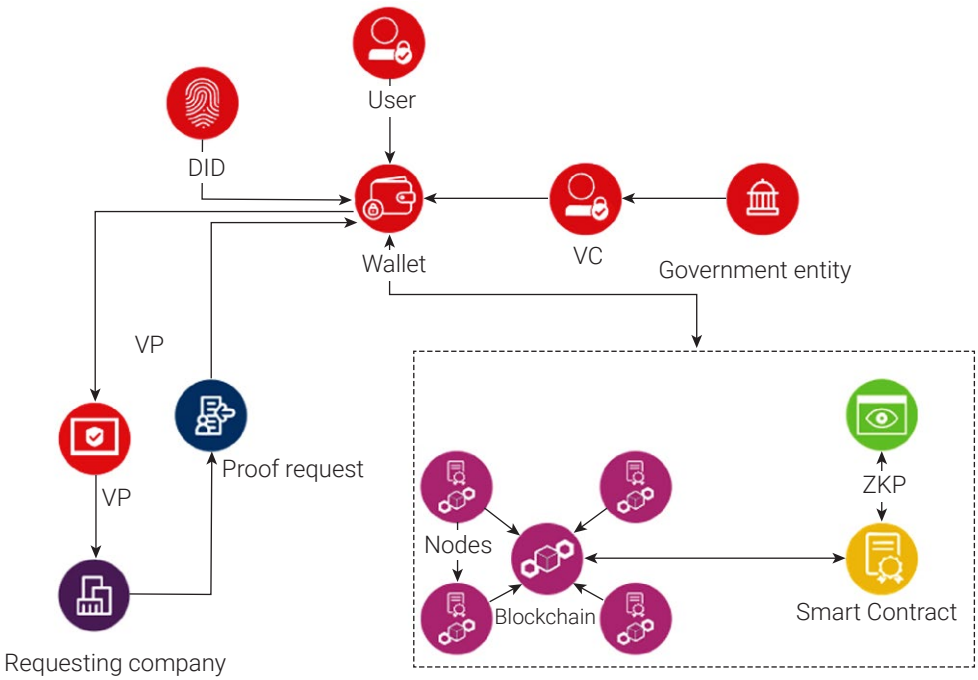


**Figure 5.** SSI implementation model on blockchain.
**Source:** Own Work

## 2.1. Model Design Based on Blockchain Technology

### *2.1.1. Creation and Management of Self-Sovereign Identity (SSI)*

Self-sovereign identity (SSI) is established through the use of a DID (Decentralized Identifier), which is a unique identifier controlled by the network user [34]. This identifier is issued through a VC (Verifiable Credential), provided by a trusted entity. In this case, the objective is to enable control of personal data at a regional level, rather than for a single organization. The proposal is oriented toward governmental entities

issuing such credentials [35], allowing their future implementation within shared technological ecosystems [36].

The proposed solution should be implemented, whenever possible, using internationally recognized standards to ensure efficiency, scalability, and long-term sustainability. For this reason, the DID would be implemented in accordance with the W3C (World Wide Web Consortium) standard, an organization dedicated to developing guidelines that enable web scalability while ensuring compatibility and interoperability with other implementations [37].

Regarding the implementation of the VC, several cryptographic standards are valid within W3C recommendations; among the most widely adopted is the JWT (JSON Web Token) standard. This approach encodes a set of values in a JSON object and validates it through a payload that contains user information and a token generated by a digital signature, thereby ensuring authenticity and integrity [38].

For the management of Decentralized Identifiers (DID) within a blockchain network, a digital wallet compatible with the Self-Sovereign Identity (SSI) model is required. Among the most relevant options for enterprise or private use is the wallet developed by Hyperledger [39]. Similarly, there are wallets compatible with public blockchain networks, such as MetaMask, Trust Wallet, and Coinbase Wallet, which are widely used in Ethereum-based environments. Additionally, solutions such as Esatus Wallet and Trinsic Wallet offer native integration with the Sovrin Foundation ecosystem.

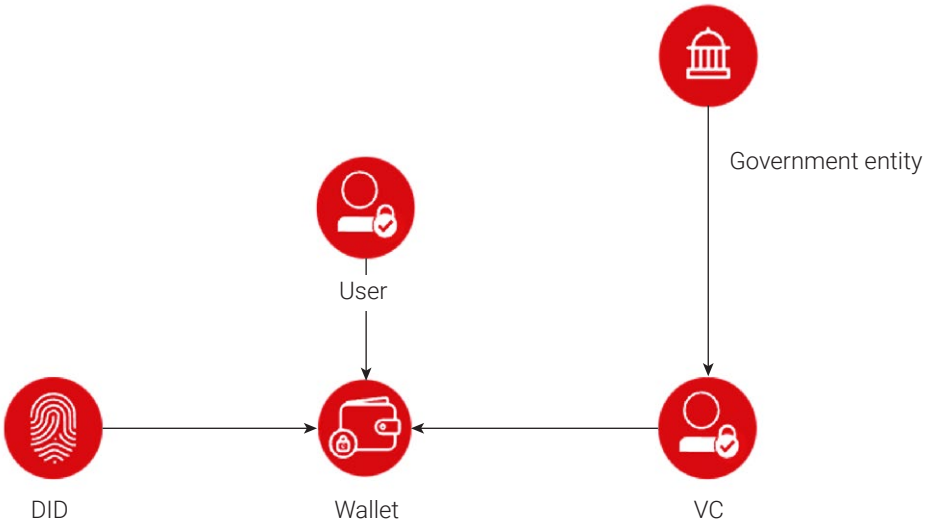


**Figure 6.** Implementation of self-sovereign identity.
**Source:** Own Work

### *2.1.2. Blockchain Ledger*

The implementation and management of SSI require a decentralized network infrastructure. Building such a network from scratch may represent a complex, time-consuming, and costly process [40]; therefore, for practical purposes, an existing standardized network that ensures trust and security in ledger management is adopted for the theoretical model.

Among the most recognized networks, three stand out:

- Hyperledger: An open-source project developed by the Linux Foundation, primarily aimed at enterprise solutions such as Hyperledger Fabric, and therefore widely used in private environments [39]. It also provides tools such as Hyperledger Aries [41], a framework for managing decentralized identities, which operates in conjunction with Hyperledger Indy, the underlying blockchain network specialized in self-sovereign identity (SSI).
- Ethereum: An open-source platform that supports decentralized blockchain networks and enables the execution of smart contracts. Ethereum has its own cryptocurrency, Ether (ETH), mainly used to perform transactions within its ecosystem [42].
- Sovrin: A global blockchain network based on Hyperledger Indy, focused exclusively on self-sovereign identity and optimized for the use of verifiable credentials and DIDs [43], [44]. Sovrin stands out for its legal and ethical framework grounded in privacy principles and compliance with personal data protection, with primary adoption in governmental contexts.

For the purposes of this work, implementation through Ethereum or Sovrin is recommended, as both projects offer continuously updated documentation and broad community support [45]. They are compatible with DID-based architectures and enable improved administrative efficiency and process consolidation within a single digital wallet. Although Hyperledger Indy, in combination with Hyperledger Aries, provides a robust solution, Sovrin builds upon this foundation by incorporating a stricter ethical and regulatory framework [46].

### *2.1.3. Smart Contracts and ZKP*

Within the Ethereum network, smart contracts function as the logical layer that enables data management and processing without intermediaries. These contracts can be integrated with Zero-Knowledge Proof (ZKP) mechanisms, as previously


e-ISSN 2357-6014 / Vol. 22, no. 2 / may-august 2026 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

discussed, providing an additional layer of privacy and security. Through this integration, it is possible to validate user attributes and credentials—for example, confirming that a user belongs to an organization or satisfies a legal requirement—without disclosing the underlying data.

In practice, ZKPs can be embedded into smart contract code as verification mechanisms without exposing raw data. Technologies such as zk-SNARKs and zk-STARKs enable the implementation of this logic within Ethereum [47]. Consequently, smart contracts not only automate the issuance and revocation of credentials but also ensure that the validation process preserves the confidentiality of personal data at the highest level, thereby strengthening user trust in decentralized systems.

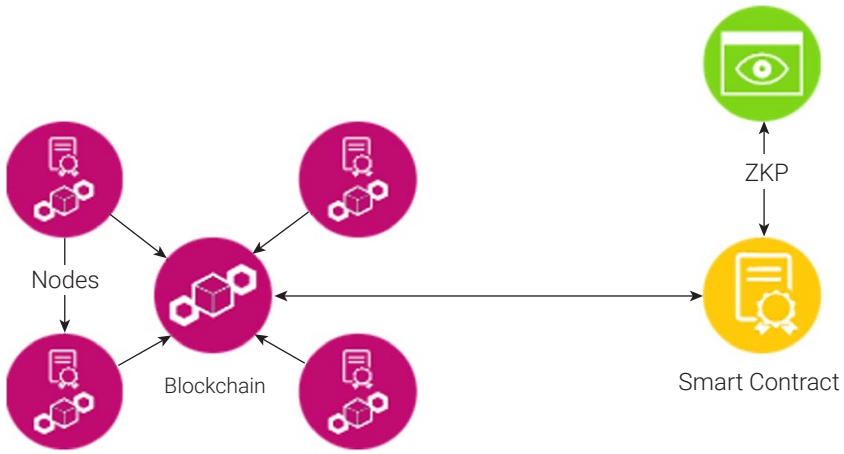


**Figure 7.** Deployment of smart contracts on a blockchain network
**Source:** Own Work

# 3. RESULTS

As a result of the analysis of the different technologies and methodologies that support user privacy, blockchain was selected as the most suitable option, as it provides the necessary capabilities:

- Decentralization: Blockchain operates through a network of decentralized nodes; therefore, information management is not confined to a single centralized location. Through a digital wallet, users can access and perform operations using their private authentication keys, while all transactions are recorded across the network nodes.

- Accessibility: The digital wallet securely stores the user's information, allowing access at any time without reliance on centralized external repositories. Access can be achieved through mobile or desktop applications with an internet connection; although some basic knowledge is required, it remains less complex than other analyzed technologies.
- Immutability and traceability: The technology enables full control over data, except for the elimination of traceability, since one of the fundamental characteristics of blockchain is its permanence over time across distributed nodes. However, it does not expose the data itself, only the recorded transactions or movements in the ledger, which ensures trust and reliability in the information.
- Control and limitation: Users can update their information and grant or revoke permissions to third parties as needed. Additionally, an extra layer of privacy can be incorporated through the implementation of ZKP, ensuring that raw data are not exposed, provided that the request supports the verification format.
- Scalability: The design can be implemented in both small- and large-scale environments, anging from autonomous institutions such as academies or microenterprises to national-level deployments within hybrid public–private ecosystems. Scalability is primarily determined by the level of implementation and intended use; however, it should be noted that increasing network size and complexity also raises computational and maintenance costs.
- Security: Through its validation mechanism based on public and private keys, blockchain provides a secure and efficient way for users to perform transactions. Additionally, the immutability of the ledger ensures that records can only be updated through consensus mechanisms such as proof of work or proof of stake, depending on the network. It also incorporates encryption standards such as AES-256, applied within digital wallets and for the protection of private keys.

## 3.1. System Operation

The user generates a self-sovereign identity (SSI) through a decentralized identifier (DID) and requests a verifiable credential (VC) from the corresponding issuing entity, which may be a governmental institution or a company, depending on the use case. This credential is subsequently stored in the user's digital wallet.


e-ISSN 2357-6014 / Vol. 22, no. 2 / may-august 2026 / Bogotá D.C., Colombia
Universidad Cooperativa de Colombia

When a third party submits a verification request via the SSI wallet, the user may deny or authorize access. If authorized, a cryptographic proof based on zero-knowledge proofs (ZKP) is generated. This proof is then validated by a smart contract on the blockchain network, without disclosing sensitive data, through a digitally signed verifiable presentation (VP). In this manner, authenticity and immutability in identity verification are ensured.

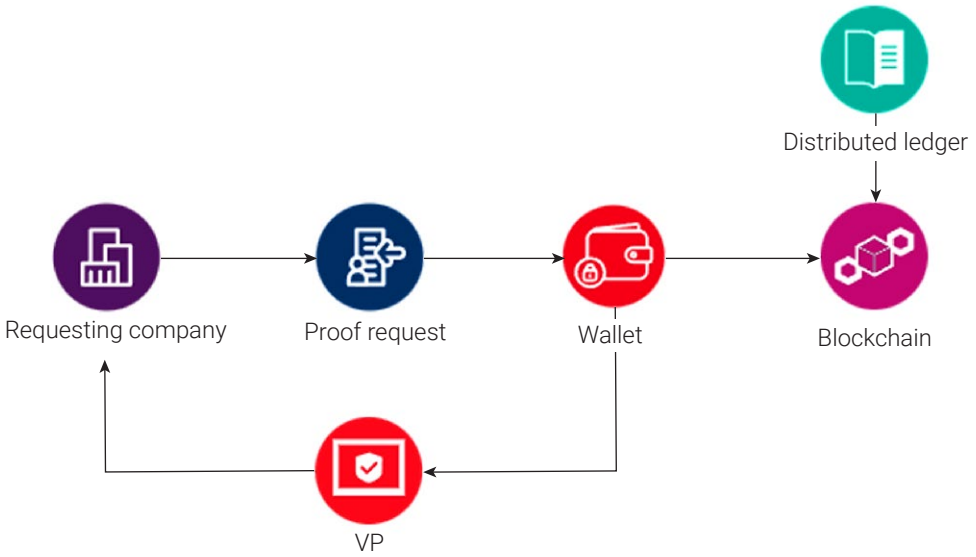


**Figure 8.** Verification request from a third party to a user.
**Source:** Own Work

## Limitations and Considerations

- Implementation requires that the selected blockchain network, as well as the technologies underlying the digital wallet, be compatible with and standardized for self-sovereign identity (SSI). Not all networks support this functionality; for example, Bitcoin [48], the most widely known blockchain network, operates as a decentralized digital currency without intermediaries, but is not suitable for the use and processing of personal data, as it is strictly focused on value transfer and transactions.
- This model is not applicable to all use cases in which third parties need to validate or access information. Certain governmental and private entities cannot operate under the proposed scheme [49], such as financial

institutions, state entities, or security organizations, since they require direct access to raw data.

- The proposed scheme requires the involvement of a public or private entity responsible for issuing digital identity certifications. This implies additional requirements and procedures inherent to the issuance process, as well as potential costs associated with network implementation [50].

# 4. DISCUSSION AND CONCLUSIONS

The comprehensive review of data protection technologies conducted in this work identified blockchain—enhanced with self-sovereign identity (SSI)—as a highly effective solution, demonstrating significant advantages for user-centered control, sovereignty, and decentralized governance of personal data. The proposed model grants users full ownership of their information, reduces dependence on third parties associated with centralization and excessive data usage, and strengthens trust in digital verification processes.

The proposed architecture demonstrates that the integration of smart contracts, ZKP, and SSI can achieve a balance between security, privacy, and usability. The implementation of a decentralized and self-sovereign structure not only impacts technical infrastructure but also redefines trust relationships among citizens, governments, and private organizations by enabling individuals to manage their credentials and perform selectively authorized verifications. However, its practical implementation will require a supporting ecosystem, preferably led by governmental institutions, to ensure the issuance of verifiable credentials and the adoption of standardized frameworks.

As future work, the development of functional prototypes based on the proposed model is recommended to validate performance, scalability, and usability. Additionally, further studies should explore its application in governmental, academic, and financial sectors, as well as define its scope and limitations within public–private environments and evaluate its short- and long-term benefits.

# REFERENCES

[1] T. Hartman, H. Kennedy, R. Steedman, and R. Jones, "Public perceptions of good data management: Findings from a UK-based survey," *Big Data & Society*, vol. 7, no. 1, pp. 2–10, 2020, doi: https://doi.org/10.1177/2053951720935616

[2] J. P. Cabrera-Sanchez and Á. F. Villarejo-Ramos, "Factors affecting the adoption of big data analytics in companies," *RAE Revista de Administração de Empresas*, vol. 59, no. 6, pp. 415–429, 2019, doi: https://doi.org/10.1590/S0034-759020190607

[3] S. Gallagher, "Equifax hackers stole data for 200k credit cards from transaction history," 2017. [Online]. Available: https://arstechnica.com/information-technology/2017/09/equifax-hackers-stole-data-for-200k-credit-cards-from-transaction-history/

[4] H. A. Rahajeng and R. A. Prastyanti, "The impact of personal data leaks on individual privacy," *Formosa Journal of Social Sciences*, vol. 4, no. 2, pp. 252–260, 2025, doi: https://doi.org/10.55927/fjss.v4i2.319

[5] W. Turton, "LastPass says hackers stole customer data, encrypted passwords," *Bloomberg.com*, 2022.

[6] R. L. Ruaro, "Algumas reflexões em torno do RGPD com alusões a LGPD," *Revista Brasileira de Direitos Fundamentais & Justiça*, vol. 14, no. 42, pp. 219–247, 2020, doi: https://doi.org/10.30899/dfj.v14i42.760

[7] J. Aguilar, "The habeas data in the last CJEU doctrine," *Teoría y Realidad Constitucional*, no. 39, pp. 557–581, 2017

[8] J. C. Gil Cifuentes, "El debido proceso en la ley de habeas data," *Revista CES Derecho*, vol. 8, no. 1, pp. 191–204, 2017, doi: https://doi.org/10.21615/cesder.8.1.10

[9] H. Jiang *et al.*, "Applications of differential privacy in social network analysis: A survey," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 1, pp. 108–127, 2023, doi: https://doi.org/10.1109/TKDE.2021.3073062

[10] N. Zafar and K. Ahmad, "Blockchain-based self-sovereign identity for ensuring traceability and provenance in online social networks," in *Lecture Notes in Networks and Systems*, vol. 1297, pp. 151–165, 2025, doi: https://doi.org/10.1007/978-981-96-3352-4_10

[11] X. Zhu, D. He, Z. Bao, M. Luo, and C. Peng, "An efficient decentralized identity management system based on range proof for social networks," *IEEE Open Journal of the Computer Society*, vol. 4, pp. 84–96, 2023, doi: https://doi.org/10.1109/OJCS.2023.3258188

[12] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "PAX: Using pseudonymization and anonymization to protect patients' identities and data in the healthcare system," *International Journal of Environmental Research and Public Health*, vol. 16, no. 9, p. 1490, 2019, doi: https://doi.org/10.3390/ijerph16091490

[13] S. Li, M. J. Schneider, Y. Yu, and S. Gupta, "Reidentification risk in panel data: Protecting for k-anonymity," *Information Systems Research*, vol. 34, no. 3, pp. 1066–1088, Sep. 2023, doi: https://doi.org/10.1287/isre.2022.1169

[14] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *Proc. IEEE Int. Conf. Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2015, pp. 57–64, doi: https://doi.org/10.1109/Trustcom.2015.357

[15] Y. Xu, W. Cui, and M. Peinado, "Controlled-channel attacks: Deterministic side channels for untrusted operating systems," in *Proc. IEEE Symposium on Security and Privacy*, 2015, pp. 640–656, doi: https://doi.org/10.1109/SP.2015.45

[16] M. A. Cardoso *et al.*, "Innovation results of IAM planning in urban water services," *Water Science and Technology*, vol. 74, no. 7, pp. 1518–1526, Jun. 2016, doi: https://doi.org/10.2166/wst.2016.291

[17] C. Singh, R. Thakkar, and J. Warraich, "IAM identity access management—Importance in maintaining security systems within organizations," *European Journal of Engineering and Technology Research*, vol. 8, no. 4, pp. 30–38, Aug. 2023, doi: https://doi.org/10.24018/ejeng.2023.8.4.3074

[18] Y. Xiao *et al.*, "Industrial experience of finding cryptographic vulnerabilities in large-scale codebases," *Digital Threats: Research and Practice*, vol. 4, no. 1, pp. 1–18, Mar. 2022, doi: https://doi.org/10.1145/3507682

[19] T. Xie, F. Liu, and D. Feng, "Fast collision attack on MD5," *Cryptology ePrint Archive*, vol. 2013, p. 170, Jan. 2013. [Online]. Available: https://eprint.iacr.org/2013/170

[20] A. Mehmood, A. Shafique, M. Alawida, and A. N. Khan, "Advances and vulnerabilities in modern cryptographic techniques: A comprehensive survey on cybersecurity in the domain of machine/deep learning and quantum techniques," *IEEE Access*, vol. 12, pp. 27530–27555, 2024, doi: https://doi.org/10.1109/ACCESS.2024.3367232

[21] S. Hohenberger and B. Waters, "Synchronized aggregate signatures from the RSA assumption," in *Lecture Notes in Computer Science*, Mar. 2018, pp. 197–229, doi: https://doi.org/10.1007/978-3-319-78375-8_7

[22] K. Krishnamoorthy and M. Jeyabalu, "A new image encryption method based on improved cipher block chaining with optimization technique," in *Advanced Image Processing Techniques and Applications*, 2017, pp. 1–17, doi: https://doi.org/10.4018/978-1-5225-2053-5.ch006

[23] I. Mazeh and E. Shmueli, "A personal data store approach for recommender systems: Enhancing privacy without sacrificing accuracy," *Expert Systems with Applications*, vol. 139, p. 112858, pp. 1–16, 2020, doi: https://doi.org/10.1016/j.eswa.2019.112858

[24] Z. Yan, G. Gan, and K. Riad, "BC-PDS: Protecting privacy and self-sovereignty through blockchains for OpenPDS," in *Proc. IEEE Int. Symp. Service-Oriented System Engineering (SOSE)*, 2017, pp. 138–144, doi: https://doi.org/10.1109/SOSE.2017.30

[25] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, 2019, doi: https://doi.org/10.1145/3298981

[26] J. Gao *et al.*, "Secure aggregation is insecure: Category inference attack on federated learning," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 1–1, Nov. 2023, doi: https://doi.org/10.1109/TDSC.2021.3128679

[27] V. Rey, P. M. Sánchez Sánchez, A. Huertas Celdrán, and G. Bovet, "Federated learning for malware detection in IoT devices," *Computer Networks*, vol. 204, p. 108693, pp. 1–14, Jan. 2022, doi: https://doi.org/10.1016/j.comnet.2021.108693

[28] Y. Wan, Y. Qu, W. Ni, Y. Xiang, L. Gao, and E. Hossain, "Data and model poisoning backdoor attacks on wireless federated learning, and the defense mechanisms: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 26, no. 3, pp. 1861–1897, Jul. 2024, doi: https://doi.org/10.1109/COMST.2024.3361451

[29] A. N. Alketbi, "Blockchain for government services – Use cases, security benefits and challenges," in *Proc. Learning and Technology Conference (LT)*, Feb. 2018, pp. 112–119, doi: https://doi.org/10.1109/LT.2018.8368494

[30] M. O. Ahmad *et al.*, "BAuth-ZKP—A blockchain-based multi-factor authentication mechanism for securing smart cities," *Sensors*, vol. 23, no. 5, p. 2757, Mar. 2023, doi: https://doi.org/10.3390/s23052757

[31] A. Badirova, F. F. Fatemi Moghaddam, and R. Yahyapour, "Integration of self-sovereign identity in centralized identity management: SSI-based authentication and attribute-based authorization," in *Proc. Int. Conf. Future Internet of Things and Cloud (FiCloud)*, 2024, pp. 362–367, doi: https://doi.org/10.1109/FiCloud62933.2024.00062

[32] T. Roth, M. Utz, F. Baumgarte, A. Rieger, J. Sedlmeir, and J. Strüker, "Electricity powered by blockchain: A review with a European perspective," *Applied Energy*, vol. 325, p. 119799, 2022, doi: https://doi.org/10.1016/j.apenergy.2022.119799

[33] D. Marchsreiter, "Towards quantum-safe blockchain: Exploration of PQC and public-key recovery on embedded systems," *IET Blockchain*, vol. 5, no. 1, pp. 1–19, Jan. 2025, doi: https://doi.org/10.1049/blc2.12094

[34] R. A. Pava-Díaz, J. I. Gil-Ruiz, and D. A. López-Sarmiento, "Self-sovereign identity on the blockchain: Contextual analysis and quantification of SSI principles implementation," *Frontiers in Blockchain*, vol. 7, p. 1443362, pp. 1–15, Jul. 2024, doi: https://doi.org/10.3389/fbloc.2024.1443362

[35] S. R. Garzon, C. Segat, and A. Küpper, "Governance of ledger-anchored decentralized identifiers," in *Proc. Crypto Valley Conference (CVC)*, 2025, pp. 44–55, doi: https://doi.org/10.1109/CVC65719.2025.00014

[36] S. Semenzin, D. Rozas, and S. Hassan, "Blockchain-based application at a governmental level: Disruption or illusion? The case of Estonia," *Policy & Society*, vol. 41, no. 3, pp. 386–401, 2022, doi: https://doi.org/10.1093/polsoc/puac014

[37] H. Halpin, "Vision: A critique of immunity passports and W3C decentralized identifiers," in *Lecture Notes in Computer Science*, vol. 12529, pp. 148–168, 2020, doi: https://doi.org/10.1007/978-3-030-64357-7_7

[38] A. Bucko, K. Vishi, B. Krasniqi, and B. Rexha, "Enhancing JWT authentication and authorization in web applications based on user behavior history," *Computers*, vol. 12, no. 4, p. 78, 2023, doi: https://doi.org/10.3390/computers12040078

[39] A. Shcherbakov, "Hyperledger Indy Besu as a permissioned ledger in self-sovereign identity," in *Lecture Notes in Informatics (LNI), Proc. Gesellschaft für Informatik (GI)*, 2024, pp. 127–137, doi: https://doi.org/10.18420/OID2024_11

[40] S. Manski, "Distributed ledger technologies, value accounting, and the self-sovereign identity," *Frontiers in Blockchain*, vol. 3, p. 29, pp. 1–12, Jun. 2020, doi: https://doi.org/10.3389/fbloc.2020.00029

[41] C. Regueiro, I. Gutierrez-Agüero, S. Anguita, S. de Diego, and O. Lage, "Protocol for identity management in industrial IoT based on Hyperledger Indy," *International Journal of Computing and Digital Systems*, vol. 12, no. 1, pp. 653–664, 2022, doi: https://doi.org/10.12785/ijcds/120153

[42] A. R. Nath, S. Bhattacharjee, and M. I. Khan, "Towards developing a decentralized identity management system with Ethereum smart contracts," in *Proc. Int. Conf. Electrical, Computer and Communication Engineering (ECCE)*, Feb. 2025, pp. 1–6, doi: https://doi.org/10.1109/ECCE64574.2025.11013086

[43] N. Naik and P. Jenkins, "Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology," in *Proc. IEEE Int. Symp. Systems Engineering (ISSE)*, 2021, pp. 1–7, doi: https://doi.org/10.1109/ISSE51541.2021.9582551

[44] P. J. Windley, "Sovrin: An identity metasystem for self-sovereign identity," *Frontiers in Blockchain*, vol. 4, p. 626726, pp. 1–14, Jul. 2021, doi: https://doi.org/10.3389/fbloc.2021.626726

[45] N. Sahi, A. Liang, W. van Devanter, K. Oikonomou, and P. Zhang, "Self-sovereign identity in semi-permissioned blockchain networks leveraging Ethereum and Hyperledger Fabric," in *Proc. Int. Conf.*, 2023, pp. 315–321, doi: https://doi.org/10.1109/ICDH60066.2023.00053

[46] A. Goel and Y. Rahulamathavan, "A comparative survey of centralised and decentralised identity management systems: Analysing scalability, security, and feasibility," *Future Internet*, vol. 17, no. 1, p. 1, Dec. 2024, doi: https://doi.org/10.3390/fi17010001

[47] P. Kumar *et al.*, "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system," *Journal of Parallel and Distributed Computing*, vol. 172, pp. 69–83, Oct. 2023, doi: https://doi.org/10.1016/j.jpdc.2022.10.002

[48] M. Fortin and E. Pimentel, "Bitcoin: An accounting regime," *Critical Perspectives on Accounting*, vol. 99, p. 102731, 2024, doi: https://doi.org/10.1016/j.cpa.2024.102731

[49] S. Mahula, E. Tan, and J. J. Crompvoets, "With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case," in *Proc. ACM Int. Conf.*, 2021, pp. 495–504, doi: https://doi.org/10.1145/3463677.3463705

[50] M. Atzori, "Blockchain technology and decentralized governance: Is the state still necessary?," *Journal of Innovation and Regulation*, vol. 12, no. 3, pp. 123–145, 2018, doi: https://doi.org/10.1234/jir.2018.12345