Blockchain and Self-Sovereign Identity: A Healthcare Use Case

Matheus Lázaro Honório da Silva[1], Gislainy Velasco[1], Noeli Antônia Pimentel Vaz[1,2], Matheus Brito Martins[1], Pedro Moraes Ribeiro Gonçalves Silva[1], Sergio T. Carvalho[1]

[1]Instituto de Informática
Universidade Federal de Goiás (UFG)

[2]Instituto Acadêmico de Ciências Exatas e Tecnológicas
Universidade Estadual de Goiás (UEG)

{matheus.lazaro, gislainycrisostomo, noelivaz}@discente.ufg.br

{matheus.b.m, pedro.ribeiro}@discente.ufg.br

sergiocarvalho@ufg.br

Abstract. *This paper proposes an architecture based on permissioned* blockchain *and self-sovereign digital identity (SSI) to address demands related to privacy, traceability, and decentralized governance in healthcare. Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) give patients greater control over their clinical data. The hybrid* on-chain/off-chain *approach enables the recording of immutable events and the management of credential issuance and verification. A functional prototype, SSISH (*Self-Sovereign Identity System for Healthcare*), demonstrates secure and interoperable workflows for examinations, diagnoses, and treatments. Preliminary results indicate increased transparency and reliability in information exchange, although further evaluation of scalability and governance in real-world environments remains necessary.*

1. Introduction

The increasing digitalization of healthcare services has enabled significant advancements, such as improved clinical data sharing among institutions and enhanced patient care. However, challenges related to privacy, security, and control over sensitive information persist because centralized systems predominantly manage this data. Such systems are vulnerable to security breaches, data leaks, and unauthorized modifications, which undermine the trust of patients and healthcare professionals [Nascimento-Silva-Junior et al. 2017]. In response, decentralized digital identity models have emerged. These models, based on Decentralized Identifiers (DIDs) and the Self-Sovereign Identity (SSI) approach, empower individuals by returning control over digital credentials and personal data to them [Reed et al. 2021].

The adoption of decentralized authentication and authorization mechanisms in healthcare seeks to minimize reliance on intermediaries, enhance interoperability, and strengthen user sovereignty over personal data. Blockchain technologies have gained prominence for their immutability, auditability, and traceability. In particular, permissioned networks like Hyperledger Fabric balance transparency and privacy while enabling federated governance and configurable consensus. Additionally, the Hyperledger Indy,

Aries, and Ursa projects provide a foundation for managing decentralized identities, facilitating the issuance and verification of Verifiable Credentials (VCs) [Allende López 2020, Santos et al. 2022].

Regulations and social demands across various countries further reinforce the realization of privacy and control over sensitive information. In Brazil, digital identity initiatives, such as e-CPF, *e-Título*, and the National Identity Document, have yet to fully unify personal documents and healthcare data [MGI 2023, Robichez et al. 2019]. Scientific evidence indicates that blockchain and SSI can provide more secure and practical solutions in this context [Bai et al. 2022, Miers et al. 2020]. Demonstrating the applicability of these approaches in healthcare can enhance patient services while mitigating risks related to data leaks, fraud, and inconsistencies in clinical records.

This work explores integrating blockchain technologies and self-sovereign digital identity (SSI) in a healthcare use case. It proposes an approach based on the Hyperledger Fabric platform for recording clinical assets and events, combined with the Hyperledger Indy, Aries, and Ursa ecosystem for managing decentralized credentials and identities. The solution is implemented by developing a functional prototype called SSISH (Self-Sovereign Identity System for Healthcare), which demonstrates the feasibility of issuing, storing, and verifying VCs related to examinations, diagnoses, and treatments, ensuring action traceability and patient privacy.

This proposal is grounded in a literature review on conceptual and technological bases of the topic, including scientific documents, W3C specifications, and repositories of relevant projects. Based on this foundation, we designed and implemented SSISH using the open-source library CC-Tools (*Chaincode Tools*) for asset development and RESTful API integration in Hyperledger Fabric, along with Aries Cloud Agent Python (ACA-Py) for credential issuance and verification.

The paper is structured into seven sections, beginning with this introduction. Section 2 explores the theoretical foundations of blockchain, decentralized digital identity, and SSI, along with related work. Section 3 details the core technologies employed – Hyperledger Fabric, Aries, Indy, and Ursa – and their integration. Section 4 presents a healthcare use case, outlining the scenario, participants, developed assets, and proposed architecture. Section 5 describes the implementation of the functional prototype. Finally, Section 7 discusses the results, conclusions, limitations, and future research directions.

2. Theoretical Foundation

2.1. Blockchain and Applications in Healthcare

Blockchain technology operates on a distributed ledger where transactions are securely stored in a chain of blocks, protected by hash functions. This structure ensures data immutability, as any attempt to modify a record disrupts the entire chain, making tampering evident [Nakamoto 2008]. Authorized participants validate and share transactions in permissioned networks like Hyperledger Fabric, enhancing privacy, access control, and shared governance among stakeholders [Burle 2019].

In the healthcare sector, blockchain supports the registration of electronic medical records, the tracking of pharmaceuticals, and the secure exchange of clinical information among institutions [Azaria et al. 2016, Robichez et al. 2019]. Its key benefits include

transparency and auditability, which help prevent fraud and ensure compliance with regulations such as Brazil's LGPD [LEI-13709 2018] and the European GDPR[1]. However, challenges remain, including scalability, data exposure on public networks, and a lack of standardization. Moreover, the development of smart contracts, particularly in public blockchain environments like the Ethereum Virtual Machine (EVM), presents several technical barriers such as language limitations, immutability constraints, and lack of development tools or accessible educational resources [Velasco et al. 2023]. In response to the challenges, researchers and developers have proposed hybrid solutions that store only metadata or hashes on the blockchain while keeping large data volumes in secure external repositories [Leite 2022]. This strategy also simplifies data correction or deletion, preventing permanent on-chain storage of full records [Wolff and Henriques 2021].

2.2. Digital Identity and SSI

Digital identity encompasses attributes and information defining a subject online, which may be a natural person, legal entity, or device [Wangham et al. 2010]. In traditional models, credential authenticity relies on centralized Identity Providers (IdPs), such as social networks or government authorities. However, this architecture creates single points of failure, is vulnerable to data breaches, and reduces user autonomy over personal information [Allen 2016].

In decentralized digital identity, specifically in Self-Sovereign Identity (SSI), users manage their credentials through a digital wallet, controlling which attributes to share and under which conditions. W3C standards, such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), reinforce this model by enabling cryptographically verifiable claims without requiring continuous interaction with the issuer [Reed et al. 2021]. Zero-Knowledge Proof (ZKP) techniques also enhance privacy by allowing users to disclose the necessary information, such as proving they are over 18 without revealing their exact date of birth [Bai et al. 2022].

A Zero-Knowledge Proof (ZKP) is an artifact combining semantic metadata, cryptographic validity, and governance rules throughout the data lifecycle. It can be inspired by the Hyperledger AnonCreds model, distinguishing three dimensions: (i) attributes disclosed for semantic interoperability (e.g., date of birth); (ii) hidden but cryptographically compromised attributes, allowing auditability without re-identification; and (iii) predicates evaluated in zero-knowledge, such as proving legal majority without revealing the exact age. These proofs can be serialized as Linked Data Proofs (W3C Verifiable Credentials Data Model 2.0[2]). The coexistence of both formats promotes interoperability and supports research on selective disclosure policies (for example, what portion of clinical data should remain verifiable, to whom, and for how long, within decentralized networks).

In healthcare, SSI offers advantages by allowing patients to store Verifiable Credentials (VCs) related to medical tests, prescriptions, and diagnoses in their digital wallets, thereby preserving privacy and reducing dependence on legacy systems. Nonetheless, challenges include the adoption of open standards, integration with electronic health records, and regulatory compliance due to the sensitive nature of healthcare data [Wolff and Henriques 2021].

[1]General Data Protection Regulation - Available at: `https://gdpr-info.eu/`

[2]`https://www.w3.org/TR/vc-data-model-2.0`

2.3. Blockchain and SSI in the Healthcare Context

The convergence of permissioned blockchain and SSI in healthcare presents opportunities to enhance data security and reliability while reinforcing patient autonomy [Nascimento-Silva-Junior et al. 2017]. Solutions based on permissioned networks that record transactions and verify credentials in a distributed manner can reduce fraud, improve traceability of treatments, and ensure the integrity of clinical information [Leite 2022].

However, large-scale adoption requires careful governance, particularly concerning the distributed ledger's ownership, validator responsibilities, participant inclusion policies, and dispute resolution mechanisms[3]. Another challenge involves managing large datasets, such as medical imaging, which are typically stored off-chain, with only references or hashes retained on the blockchain [Mello et al. 2022].

Despite recent advances in integrating blockchain and SSI, deploying and managing decentralized identity infrastructures (mainly using platforms like Hyperledger Indy) remains complex and error-prone, especially in healthcare environments where privacy and interoperability are critical. The manual configuration of nodes, cryptographic setup, and operating system dependencies imposes a significant technical barrier to adoption. To address this challenge, the MinIndy framework [Veloso et al. 2024] offers an automated solution for deploying and managing Indy networks using tools like Ansible and Docker, reducing the operational burden without compromising performance. This type of automation can facilitate the adoption of decentralized identity in healthcare institutions with limited technical expertise.

Furthermore, orchestrating decentralized identity agents is key to operationalizing SSI infrastructures based on Hyperledger Indy. Solutions like Aries Cloud Agent Python (ACA-Py) enable interaction with the Indy ledger through DIDComm protocols[4], automating tasks such as DID registration, credential issuance, and proof verification. These agents expose APIs that simplify integration with external systems and support multitenancy, which is essential for healthcare applications involving multiple institutions. The Janus system [Gomes et al. 2024] demonstrates how ACA-Py agents can manage Verifiable Credentials even in constrained environments, reinforcing the applicability of agent-based architectures in secure and privacy-preserving healthcare scenarios.

2.4. Related Work

Several recent studies have explored the convergence of blockchain and digital identity technologies, with emerging applications in healthcare. Nascimento et al. [Nascimento-Silva-Junior et al. 2017] discuss protecting sensitive healthcare data, emphasizing the importance of robust technological solutions to ensure privacy and trust among stakeholders. Although the study highlights blockchain's role in mitigating data leaks and fraud risks, it does not address the integration with self-sovereign digital identity models.

In a broader context, Robichez et al. [Robichez et al. 2019] analyze the use of blockchain in governmental scenarios, focusing on citizen identification solutions. While

[3]Hyperledger Fabric Documentation: `https://hyperledger-fabric.readthedocs.io`

[4]DIDComm Messaging v2.x Editor's Draft: `https://identity.foundation/didcomm-messaging/spec/`

acknowledging the potential of these technologies to enhance public system security and transparency, the authors do not explore aspects of self-sovereign identity or its specific applicability to healthcare. Similarly, Leite and Henriques [Leite 2022] examine the transition from federated to decentralized identity models, emphasizing privacy and user control benefits. However, their study remains conceptual and does not provide a concrete application for managing clinical data.

Within institutional research, Wolff and Henriques [Wolff and Henriques 2021] examine the adoption of SSI by Brazil's National Education and Research Network (RNP), focusing on technical and governance aspects in academic settings. Although providing valuable insights into SSI implementation, the study does not address the particularities of the healthcare sector, especially regarding the handling of clinical Verifiable Credentials (VCs) and their integration into care workflows.

Other technical proposals include using smart contracts and blockchain-based access control models, as presented by Vora et al. [Vora et al. 2018] and Xu et al. [Xu et al. 2019]. These authors propose architectures for managing electronic health records and consent in decentralized networks. Despite the value of mechanisms promoting traceability and integrity, the proposed solutions do not fully incorporate SSI principles, such as DIDs, digital wallets, or Verifiable Credentials (VCs), limiting the end user's control over personal information.

In contrast to the studies mentioned above, this paper proposes effectively integrating a permissioned blockchain (Hyperledger Fabric) with the Hyperledger Indy, Aries, and Ursa ecosystem, emphasizing self-sovereign digital identity in healthcare. The proposed solution, SSISH, encompasses both immutable clinical event recording and the issuance and verification of Verifiable Credentials (VCs) through digital wallets. In addition to ensuring auditability and interoperability, the model offers patients granular control over their data, combining selective privacy, explicit consent, and cryptographic verification.

3. Core Technologies Used

This section details the main technological components employed in the proposed infrastructure, with an emphasis on the integration of the Hyperledger Fabric permissioned blockchain network, the decentralized identity ecosystem composed of Hyperledger Indy, Aries, and Ursa, and supporting tools such as the CC-Tools library. This technological foundation enables the traceability of clinical events and the management of digital identities and Verifiable Credentials (VCs), as described in Section 4.

3.1. Hyperledger Fabric and the Use of CC-Tools

Hyperledger Fabric is a permissioned blockchain platform maintained by the Linux Foundation under the Hyperledger project, aimed at enterprise applications with privacy and shared governance requirements [Burle 2019]. Fabric adopts the execute-order-validate model for transaction processing. Initially, a set of endorsers simulates the chaincode and generates a read/write set. Subsequently, the ordering service organizes transactions into blocks, and finally, each peer validates and applies the transactions to the ledger, provided they remain valid.

To facilitate solution development on Fabric, the open-source library CC-Tools (Chaincode Tools)[5] was used. CC-Tools provides a high-level abstraction for modeling assets and transactions, including CRUD operations, event logging, metadata control, and automatic exposure of a RESTful API (`cc-api`). This abstraction enables external applications to interact with the network without the complexity of directly using the Fabric SDK. In the proposed system, CC-Tools was used to define assets such as *Exam*, *Diagnosis*, and *Treatment*, which are associated with access control rules, versioning, and auditability.

3.2. Hyperledger Indy, Aries, and Ursa

In addition to Fabric, the SSISH infrastructure integrates the Hyperledger ecosystem for decentralized identity, which is composed of the Indy, Aries, and Ursa projects. Hyperledger Indy[6] provides the Indy Ledger, a blockchain network specifically designed to register Decentralized Identifiers (DIDs), credential schemas, and credential definitions. This foundation enables the secure and interoperable issuance and verification of Verifiable Credentials (VCs) [Reed et al. 2021]. Despite being perceived by some as stagnant after 2022, the 2024 Annual Review reaffirmed Hyperledger Indy's *graduated* status, citing six years of uninterrupted Sovrin MainNet uptime and a 20% growth in contributors (46 individuals) since 2022[7].

Hyperledger Aries defines the communication protocols between identity agents, through the Aries RFCs, enabling credential exchange, cryptographic proof sharing, and peer-to-peer relationships among digital wallets. Hyperledger Ursa[8] provides cryptographic libraries that support functionalities such as Zero-Knowledge Proofs (ZKPs), strengthening the security and privacy of interactions. In practice, the proposed system uses ACA-Py (Aries Cloud Agent Python)[9], which implements Aries RFCs and performs the operations of registering, issuing, and verifying Verifiable Credentials (VCs) on the Indy Ledger [Mello et al. 2022].

3.3. Integration in SSISH

The SSISH (Self-Sovereign Identity System for Healthcare) proposal integrates Hyperledger Fabric with the Indy, Aries, and Ursa ecosystems. Fabric manages the recording of clinical assets and events in a permissioned network with distributed governance. At the same time, the Aries/Indy handles the issuance, storage, and verification of digital credentials associated with individuals or institutions. We developed the architecture with a Vue.js front-end and a Node.js back-end, which connects two key components: (i) the CC-Tools RESTful API for asset registration and queries on Fabric, and (ii) the ACA-Py agent, which interacts with the Indy Ledger to manage DID and VCs [Venzi et al. 2025].

[5]Repository available at: `https://github.com/hyperledger-labs/cc-tools-demo`

[6]Hyperledger Indy Overview: `https://lf-hyperledger.atlassian.net/wiki/spaces/indy/overview`

[7]2024 Annual Review - Hyperledger Indy: `https://toc.hyperledger.org/project-reports/2024/2024-annual-Hyperledger-Indy.html`

[8]Hyperledger Ursa (EOL) Overview: `https://lf-hyperledger.atlassian.net/wiki/spaces/ursa/overview`

[9]Aries Cloud Agent Python Documentation: `https://aries-cloud-agent-python.readthedocs.io/en/latest`

This configuration empowers patients to control their credentials, selectively sharing them with healthcare institutions through cryptographic proofs and explicit consent.

Among the components used, the *Traction*[10] project stands out. It is an open-source initiative maintained by the Government of British Columbia that provides a digital wallet built on Hyperledger Aries Cloud Agent Python. Traction simplifies credential issuance and receipt workflows by abstracting the technical configuration details of the agent, adopting an API-first and multitenant approach that supports scalability and integration with existing systems. The implementation of SSISH follows this model, leveraging both the front-end structure and the ACA-Py core as references.

4. Use Case: SSISH – Self-Sovereign Identity System for Healthcare

4.1. Scenario and Stakeholders

The SSISH system can be illustrated, in its conceptual form, as a healthcare environment involving multiple stakeholders: (*i*) **Ana**, a patient who wishes to maintain control over her health data, such as examinations, diagnoses, and treatments; (*ii*) **Dr. Carlos**, a physician responsible for issuing health-related credentials; (*iii*) **Laboratories** and **Clinics**, which may issue test results; and (*iv*) **Insurance Companies and Other Institutions**, which may verify these credentials. The patient uses a digital wallet (BC Wallet), based on Aries/Indy, to receive, store, and share credentials as needed [Wolff and Henriques 2021].

After Ana undergoes an examination, a laboratory generates a report, which she stores in a secure repository using MinIO[11]. The report's hash or reference is then stored on the Fabric blockchain. Aries/Indy issues the credential associated with the report, which Ana receives in her digital wallet. When Dr. Carlos needs to evaluate the report, he requests the credential presentation, which is cryptographically verified using Zero-Knowledge Proofs to ensure authenticity and privacy [Bai et al. 2022].

4.2. Operational Workflow

The typical operational workflow consists of: (1) creation or registration of a digital wallet by a patient or professional; (2) registration of the examination in Fabric (defining an *Exam* asset); (3) issuance of a Verifiable Credential (e.g., *ExamVC*) using ACA-Py; (4) reception and storage of the credential in the patient's digital wallet; (5) selective presentation of the report to a verifier using Aries and ZKP-based verification; and (6) recording of each event on the Fabric blockchain, which serves as an immutable audit trail [Leite 2022, Venzi et al. 2025].

Figure 1 provides a simplified illustration of the credential issuance and verification process in a healthcare environment, highlighting the integration between the Hyperledger Fabric network (for asset and event registration) and Aries/Indy (for DID and Verifiable Credential management). Using hashes and metadata, rather than entire report contents, preserves patient privacy while ensuring traceability, as only credential holders can grant access to the complete information.

[10]More details at: `https://github.com/bcgov/traction`

[11]Object storage system used as a repository for clinical files: `https://min.io/docs/minio/linux/index.html`

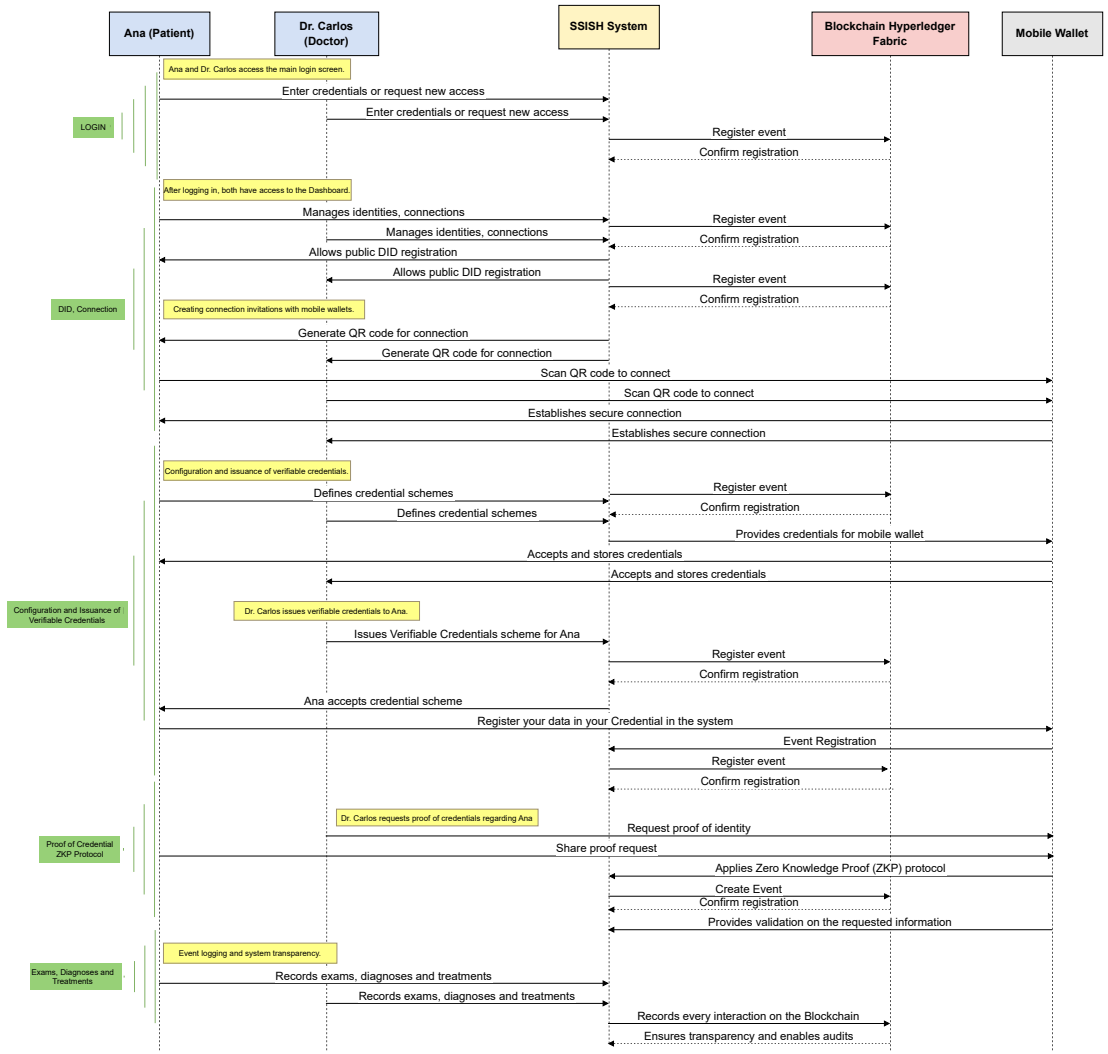

Figure 1. Credential issuance and verification workflow in SSISH, involving the actors Ana and Dr. Carlos. Entities communicate using blockchain and the Aries/Indy ecosystem.

4.3. SSISH Architecture

The SSISH architecture, shown in Figure 2, comprises three main layers. The SSISH layer provides the user interface and business logic for issuing, storing, and verifying digital credentials. The second is the blockchain layer, implemented with Hyperledger Fabric, composed of three participating organizations, a RESTful API exposed via `cc-api`, and the chaincodes responsible for asset and transaction registration in the permissioned network. Finally, the architecture includes an off-chain storage layer, composed of databases such as the Endorser DB, Postgres SSISH DB, and the MinIO service, which securely store metadata, hashes, and other significant clinical data that are not persisted directly on the blockchain.

This modular structure favors scalability and the inclusion of new services or participants in the network, ensuring privacy and efficiency in health data processing.

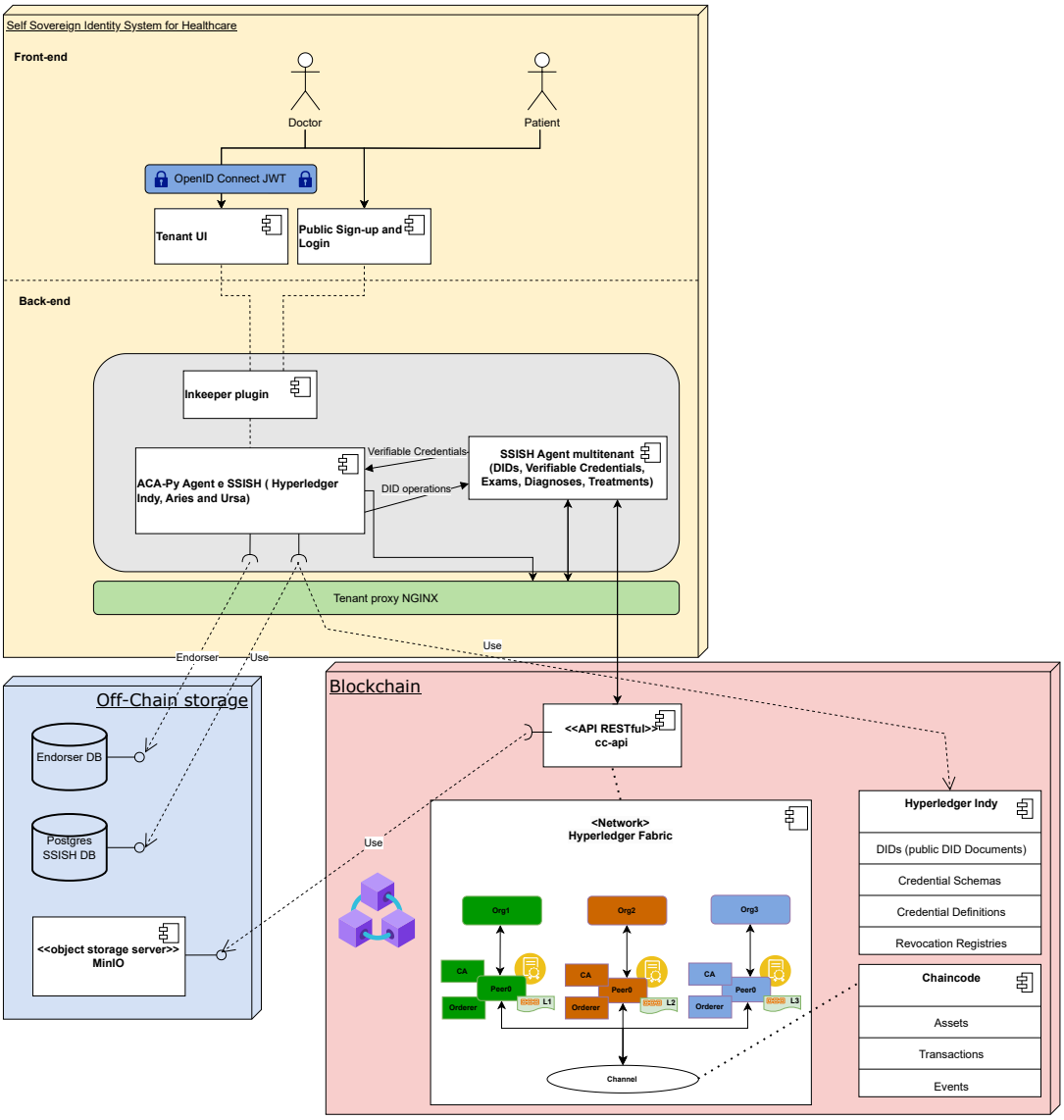

Figure 2. SSISH architecture diagram.

4.4. Entities and Implemented Assets

Figure 3 presents the asset diagram adopted by SSISH on the Hyperledger Fabric platform. Each asset represents an entity or fundamental resource for decentralized control of clinical data and digital credentials in healthcare.

The main implemented assets include: *Exam*, *Diagnosis*, and *Treatment* objects, representing medical examinations, diagnoses, and treatments associated with a patient, which may be related to one another according to the care flow logic; the *Digital Wallet*, linked to either a patient or a healthcare professional, responsible for storing DIDs and VCs; the *VerifiableCredential* and *DID* assets, which form the basis of self-sovereign digital identity, describing the issuer, holder, and cryptographic verification parameters; and finally, the *SSISHEvent* and *CredentialVerification* assets, which register relevant system events on the blockchain, such as credential verifications, forming a reliable, immutable,

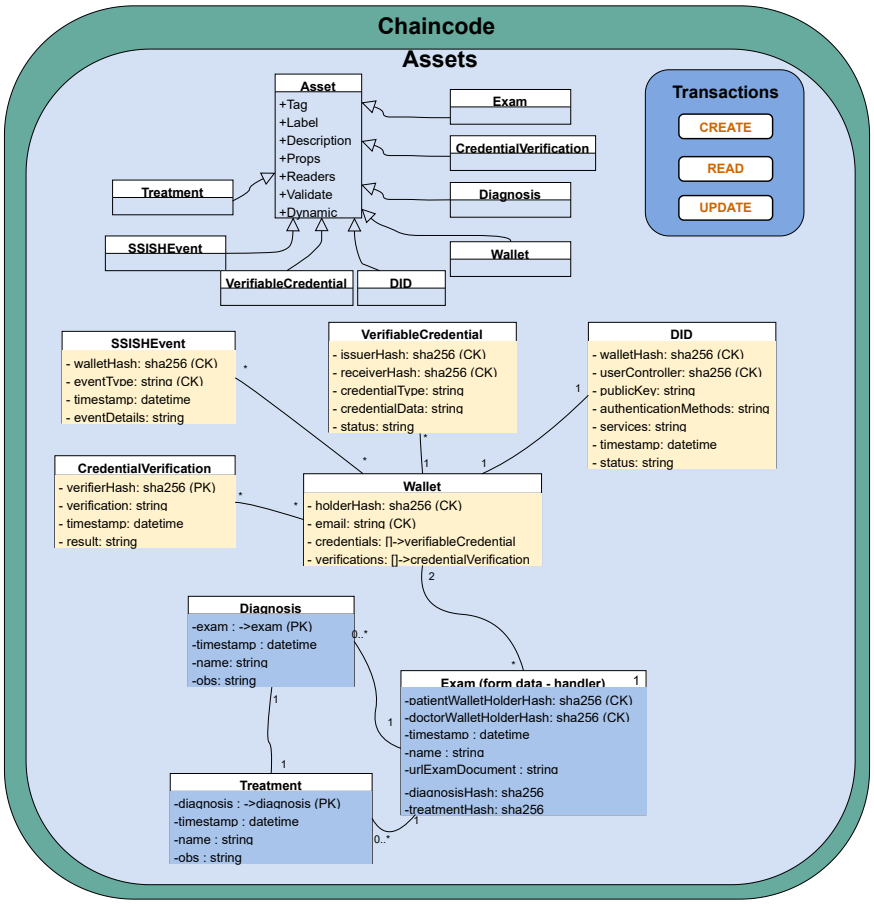

Figure 3. Asset diagram in Hyperledger Fabric.

and verifiable audit trail. Operations such as *CREATE*, *READ*, and *UPDATE* enable the system to manage assets, while additional functions like *ReadAssetHistory* and *Search* allow for historical tracking and specific queries on the ledger.

5. The Developed Prototype

SSISH was implemented as a functional prototype to validate the proposed integration between blockchain and self-sovereign digital identity technologies in healthcare. The complete source code is publicly available in two repositories under the organization "SelfSovereignIdentity-SystemHealthcare" on GitHub: `SSISH-SSISystem`[12] and `SSISH-Blockchain Hyperledger Fabric`[13]. These repositories provide installation scripts, custom chaincodes, and RESTful endpoints, enabling the replication of the environment. The solution requires adaptation to different scenarios.

The development environment runs on Ubuntu 22.04.1 LTS, where we installed all necessary dependencies, including Git, Curl, JQ, Docker (v24.0.5), Docker Compose (v1.29.2), Node.js (v12.18.2), npm (v6.14.5), and GoLang (v1.14.3). We configured the

[12] `https://github.com/SelfSovereignIdentity-SystemHealthcare/SSISystem`

[13] `https://github.com/SelfSovereignIdentity-SystemHealthcare/blockchainFabric-SSISH`

Hyperledger Fabric network using the CC-Tools tool, which streamlined the definition of assets and transactions and enabled the exposure of a RESTful API via `cc-api`. Concurrently, we employed the Aries Cloud Agent Python (ACA-Py) to manage DIDs and to issue and verify VCs on the Indy Ledger.

Figure 4 provides an overview of the prototype interface, highlighting four main functionalities: (*a*) authentication via the digital wallet; (*b*) issuance and reception of credentials; (*c*) user dashboard with interaction history and available credentials; and (*d*) credential registration through the mobile wallet. These interfaces demonstrate the integration between Hyperledger Fabric and the Aries/Indy ecosystem, enabling patients and healthcare professionals to control their data and share sensitive information securely and verifiably. Each credential can be cryptographically verified anytime, ensuring selective privacy, traceability, and explicit consent.

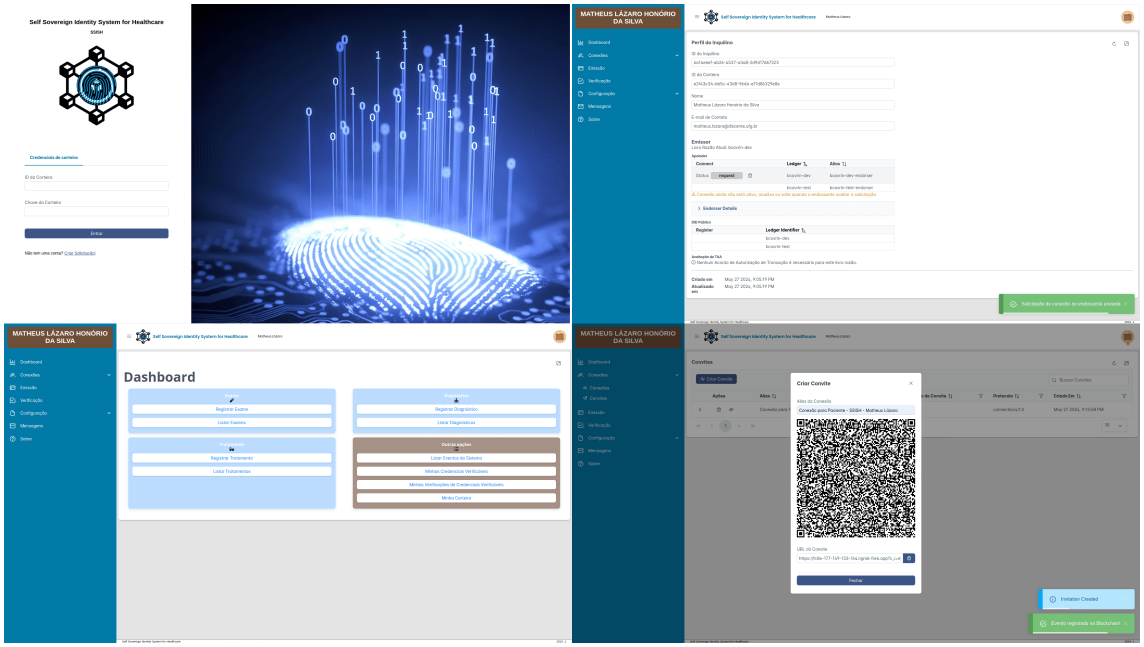

Figure 4. Prototype demonstration: (a) Login using digital wallet (top left), (b) Credential issuance (top right), (c) Dashboard view (bottom left), and (d) Credential registration via mobile wallet (bottom right).

6. Results and Discussion

SSISH was developed as a functional prototype and evaluated in a controlled environment, demonstrating the feasibility of combining a permissioned blockchain (Fabric) with SSI technologies (Aries, Indy, and Ursa) to enhance privacy and control over sensitive data. Preliminary performance tests indicate that Fabric chaincodes and credential issuance and verification via Aries/Indy do not cause significant delays in small-scale scenarios. However, further testing is necessary to confirm scalability in more complex environments. Additionally, the generation and verification of Verifiable Credentials (VCs), coupled with event traceability on the ledger, offer promising opportunities for innovation in healthcare services by reinforcing the security of data sharing and the suitability of records.

From a user experience perspective, the digital wallet clarifies who holds or requests a clinical record by removing intermediaries during authentication. Self-

sovereign identities simplify processes and lower fraud risk, as patients control data sharing [Allen 2016, Nascimento-Silva-Junior et al. 2017, Wolff and Henriques 2021]. The SSISH implementation also shows that confidentiality is preserved by storing clinical files off-chain and recording only metadata or hashes on the blockchain, preventing unauthorized access and ensuring version control and historical integrity.

However, this discussion still lacks validation in real-world scenarios, where factors such as the diversity of legacy systems and regulatory compliance may impact implementation. Additionally, the learning curve for using digital wallets and DIDs requires specific training, demanding the mobilization of multiple stakeholders in the sector.

Beyond the prototype's main flow, the architecture supports exploratory scenarios reflecting key clinical challenges. One example is access revocation: when a patient changes their primary physician, the previous provider's DID could be removed from the ledger's access control list, automatically restricting access to records. Another scenario involves insurers, who may request zero-knowledge proofs confirming a diagnosis eligible for coverage without revealing the ICD code[14]. Public authorities could also perform aggregated audits (e.g., vaccination counts) using anonymized blockchain events, preserving privacy while gathering epidemiological data. Though not yet implemented in SSISH, these cases suggest the model's potential as a foundation for research on lifecycle governance (covering issuance, presentation, revocation, and archiving) within distributed healthcare ecosystems.

7. Conclusion

This work presented SSISH, which integrates Hyperledger Fabric with the self-sovereign digital identity ecosystem (Indy, Aries, and Ursa) for healthcare applications. The results demonstrated that the integration of permissioned blockchain with SSI allows for the secure and traceable registration and retrieval of clinical events. At the same time, the issuance of Verifiable Credentials (VCs) ensures that only credential holders share their data with authorized parties. This architecture shows potential to increase trust and improve privacy, while also promoting interoperability.

Nevertheless, we acknowledge certain limitations that may affect large-scale adoption. SSISH remains a prototype and has not yet been validated in real-world environments, leaving open issues related to performance, governance, network orchestration, and integration with legacy systems. Additionally, the absence of broader standardization may hinder interoperability with electronic medical records and governmental repositories, necessitating regulatory adaptations and institutional agreements. Despite these challenges, the results support the proposed model's feasibility and encourage further research to explore its application in broader scenarios.

Future work may address scalability by evaluating performance under scenarios with higher data volumes and transaction loads and exploring advanced Zero-Knowledge Proof techniques to enhance selective privacy. The aim is to develop mature governance strategies by integrating distributed governance, participation policies, and dispute resolution mechanisms to foster broader adoption across diverse healthcare environments.

[14]International Classification of Diseases maintained by the World Health Organization (WHO): `https://www.who.int/standards/classifications/classification-of-diseases`.

References

Allen, C. (2016). The path to self-sovereign identity. *Life with Alacrity*.

Allende López, M. (2020). Self-sovereign identity: The future of identity: Self-sovereignity, digital wallets, and blockchain.

Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30.

Bai, T., Hu, Y., He, J., Fan, H., and An, Z. (2022). Health-zkidm: A healthcare identity system based on fabric blockchain and zero-knowledge proof. *Sensors*, 22(20).

Burle, L. M. (2019). Um estudo de caso em cadeias de blocos: principais mecanismos de consenso e a plataforma hyperledger fabric. Available at: https://app.uff.br/riuff/bitstream/handle/1/12585/Trabalho_de_Conclus_o_de_Curso_LeonardoMBurle.pdf?sequence=1&isAllowed=y. Accessed on: 19 mar. 2025.

Gomes, A., Sousa, A., Estevam, V., Lazzarin, E., and Lima, L. (2024). Janus: A tool for managing identities for iot agents using verifiable credentials. In *Anais Estendidos do XLII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 253–258, Porto Alegre, RS, Brasil. SBC.

LEI-13709 (2018). Lei nº 13.709, de 14 de agosto de 2018. dispõe sobre a proteção de dados pessoais e altera a lei nº 12.965, de 23 de abril de 2014 (marco civil da internet). Available at: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed on: 19 mar. 2025.

Leite, Raquel Pereira e Henriques, M. A. A. (2022). Estudo sobre a transição entre gestão de identidades digitais federadas e distribuídas. Available at: https://www.prp.unicamp.br/inscricao-congresso/resumos/2022P20346A3750303517.pdf. Accessed on: 19 mar. 2025.

Mello, E. R. d., Chaves, S. A. d., Silva, C. E. d., Wangham, M. S., Brito, A., and Henriques, M. A. A. (2022). Autenticação e autorização: antigas demandas, novos desafios e tecnologias emergentes. In *XXII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg 2022)*, chapter 1. Accessed on: 19 mar. 2025.

MGI, P. G. (2023). Carteira de identidade nacional. Available at: https://www.gov.br/governodigital/pt-br/identificacao-do-cidadao. Accessed on: 19 mar. 2025.

Miers, C. C. et al. (2020). Blockchains com hyperledger: conceitos, instalação, configuração e uso. Available at: https://errc.sbc.org.br/2020/mc/Texto_Minicurso_ERRC_2020_Hyperledger_Fabric.pdf. Accessed on: 19 mar. 2025.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf.

Nascimento-Silva-Junior, D., Lima-De-Araujo, J., and Gurgel-Cosme-Do-Nascimento, E. (2017). Privacidade e confidencialidade no contexto mundial de saúde: uma revisão integrativa. *Rev. Bioética y Derecho*, pages 195 – 214.

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., and Sabadello, M. (2021). Decentralized identifiers (dids) v1.0 - core architecture, data model, and representations. Available at: https://www.w3.org/TR/did-core/. W3C Working Draft.

Robichez, G., Frajhof, I., Alves, P. H., Nasser, R., Paskin, R., and Fiorini, S. (2019). Blockchain para governos e serviços públicos. Available at: https://bib-di.inf.puc-rio.br/ftp/pub/docs/techreports/19_01_robichez.pdf. Accessed on: 19 mar. 2025.

Santos, C. R. P. d., Priesnitz Filho, W., Gonçalves, P. A. d. S., and Henke, M. (2022). Xxii simpósio brasileiro de segurança da informação e de sistemas computacionais [recurso eletrônico] : Minicursos do sbseg 2022. Available at: https://sol.sbc.org.br/livros/index.php/sbc/catalog/view/107/481/754-1. Accessed on: 19 mar. 2025.

Velasco, G., Vaz, N., and Carvalho, S. (2023). Challenges and opportunities in smart contract development on the ethereum virtual machine: A systematic literature review. In *Anais do VI Workshop em Blockchain: Teoria, Tecnologias e Aplicações*, pages 15–28, Porto Alegre, RS, Brasil. SBC.

Veloso, A., Sousa, J., Evaristo, B., Abreu, D., Saraiva, F., and Abelém, A. (2024). Minindy: Um framework para automatizar a implantação e o gerenciamento de redes blockchain hyperledger indy. In *Anais do VII Workshop em Blockchain: Teoria, Tecnologias e Aplicações*, pages 55–68, Porto Alegre, RS, Brasil. SBC.

Venzi, S., Macedo, A., Fernandes, M., Andreghetti, B., GoLedger, Campelo, L., Lermen, A., Lázaro, M., Magdy, O., and Pereira, J. (2025). cc-tools-demo: Exemplo de uso da biblioteca *cc-tools* para desenvolvimento de *chaincodes* com apis restful no hyperledger fabric. https://github.com/hyperledger-labs/cc-tools-demo. Acesso em: 26 mar. 2025.

Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., and Rodrigues, J. J. P. C. (2018). Bheem: A blockchain-based framework for securing electronic health records. In *2018 IEEE Globecom Workshops (GC Wkshps)*, pages 1–6.

Wangham, M. S., Mello, E. R. d., et al. (2010). Gerenciamento de identidades federadas. In *MINICURSOS X Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*. Accessed on: 19 mar. 2025.

Wolff, B. and Henriques, M. (2021). Estudo experimental sobre gestão de identidades autossoberanas para avaliação de riscos e oportunidades de adoção pela rnp. Available at: https://sol.sbc.org.br/livros/index.php/sbc/catalog/view/107/481/754-1.

Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., and Yu, N. (2019). Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. *IEEE Internet of Things Journal*, 6(5):8770–8781.