





ORIGINAL RESEARCH

# Soulbound Tokens: Enabler for Privacy-Aware and Decentralized Authentication Mechanism in Medical Data Storage

Biagio Boi, PhD , Student; Franco Cirillo, PhD , Student; Marco De Santis, PhD , Student; and Christian Esposito, PhD 

Department of Computer Science, University of Salerno, Fisciano, Italy

Corresponding Author: Franco Cirillo, Email: [fracirillo@unisa.it](mailto:fracirillo@unisa.it)

DOI: <https://doi.org/10.30953/bhty.v7.334>

Keywords: authentication, blockchain, healthcare, medical record, SBT, Self-Sovereign Identity, Soulbound Token, SSI

## Abstract

---

**Context:** The digitalization of the healthcare sector faces significant challenges due to the diverse representation of data and their distribution across various hospitals. Moreover, security is a key concern as healthcare-related data are subject to the legal obligations of General Data Protection Regulation (GDPR) and similar data protection legislation. Standardization efforts like Health Level Seven (HL7) have been implemented to enhance data interoperability. However, authentication still remains a critical issue with significant challenges.

**Aim:** This research aims to improve and strengthen the authentication process by introducing a novel architecture for decentralized authentication. Additionally, it proposes a new approach to decentralized data management, which is crucial for handling sensitive medical data efficiently.

**Methodology:** The proposed architecture adopts a user-centric approach, utilizing Self-Sovereign Identity (SSI). It introduced a new non-fungible token (NFT) type called soulbound token (SBT) in the medical context, which will facilitate user authentication across different hospitals, effectively creating a federation of interconnected institutions.

**Results:** The implementation of the proposed architecture demonstrated a significant reduction in authentication time across multiple hospitals. The use of SBT ensured secure and seamless user authentication, enhancing overall system interoperability and data security. The decentralized approach also mitigated the risks associated with centralized authentication servers.

**Conclusion:** This study successfully presents a novel decentralized authentication architecture for the healthcare domain, leveraging SSI and SBTs. This approach accelerates the authentication process and enhances data security and interoperability among hospitals. Future research should explore the scalability of this architecture and its application in other sectors requiring stringent data security measures.

## Plain Language Summary

This research addresses challenges in digital healthcare, particularly in data variety, distribution, and authentication. It introduces a decentralized authentication system using Self-Sovereign Identity and a new type of non-fungible tokens called soulbound tokens. This system links hospitals, reduces authentication times, enhances data security, and improves system interoperability. By decentralizing authentication, it mitigates risks associated with centralized servers. This study results suggest that this innovative approach could benefit healthcare and potentially other industries with stringent data security needs, though further research on scalability and broader applications is recommended.

---

Submitted: July 2, 2024; Accepted: August 9, 2024; Published: August 31, 2024

Improving data management, operational effectiveness, and patient care, all depend on the healthcare industry going digital. However, there are several major obstacles to this shift, especially when it comes to authentication and data compatibility. Healthcare data are often dispersed throughout several systems and organizations,<sup>1</sup> each of which uses a different set of standards and technology to manage patient data. This fragmentation makes it difficult to integrate across different systems and causes discrepancies in data representation. The absence of a standard data format makes data interchange more difficult and increases the risk of errors and inefficiencies. Because many systems do not always work well together, users could have trouble easily accessing their health records. This disarray compromises the effectiveness of care coordination and could lead to mistakes or delays in patient care.

Conventional healthcare authentication methods usually depend on centralized servers to store and validate user credentials. These centralized systems have several difficulties, such as:

- **Single Point of Failure:** Centralized servers used for authentication are prone to malfunctions. The entire network may be affected if the server fails or is compromised, making it impossible for staff members at different institutions to access patient data.
- **Scalability Issues:** As healthcare networks develop and their user base increases, centralized systems may not be able to keep up with the demand, which could result in performance bottlenecks.
- **Cybersecurity-related Risks:** Centralized servers are frequently the focus of cyberattacks. If an attack on these systems is successful, critical patient data may be compromised in massive data breaches.

Reliance on centralized authentication systems may lead to serious security flaws that compromise the overall effectiveness and security of healthcare data management. This vulnerability is exacerbated in a decentralized environment where data are spread across various institutions.

Strict laws like the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) apply to healthcare data. To safeguard patient privacy and guarantee compliance, these regulations impose strict controls over data access and management. Conventional authentication methods frequently fail to strike a compromise between user ease and security. Complicated authentication standards may result in more administrative work and possible noncompliance. For traditional systems, it is difficult to guarantee that only authorized personnel will access important information while preserving a seamless user experience.

The complexity of healthcare data networks is increasing along with the number of users, and existing authentication solutions might not be able to keep up.<sup>2</sup> Several conventional systems are based on inflexible infrastructures that make it difficult to modify them in response to changes in the healthcare industry or in technology. It is possible that old authentication techniques will become obsolete or require expensive modifications as healthcare systems develop and incorporate new technologies. This lack of flexibility and scalability may make it more difficult for the industry to develop and adapt to new problems.

This research aims to address the authentication challenges in the healthcare sector by proposing a novel decentralized authentication architecture. The proposed solution leverages self-sovereign identity (SSI), a user-centric approach that empowers an individual's control over their digital identities. Additionally, the architecture introduces a new type of non-fungible token (NFT) known as the soulbound token (SBT). The SBTs are a specific type of non-transferable token introduced to represent personal credentials and achievements on the blockchain in a secure and verifiable manner.

Unlike traditional fungible tokens or transferable NFTs, SBTs are bound to a specific individual and cannot be transferred or traded to another party. The origin of SBTs lies in the need for a reliable method to digitally represent and verify personal attributes and credentials such as academic degrees, professional certifications, and membership records. This need has become more pressing as human verification gains importance in various domains, from education to professional networking and beyond. The term "soulbound" metaphorically represents the idea that these tokens are inherently linked to the individual's "soul," meaning their personal and unique identity, and are not meant to be detached or exchanged. By implementing this decentralized approach, we aim to create a federated network of healthcare institutions, enhancing data security and interoperability while significantly reducing authentication times. To complement this decentralized authentication architecture, we propose the integration of a Solid data management system (a medium for the secure, decentralized exchange of public and private data), which provides a robust framework for decentralized data storage and management. By utilizing Solid, patients can store their personal health data in personal online data stores (Pods), which they fully control. This ensures that patients have the authority to grant or revoke access to their health information, fostering trust and enhancing privacy.<sup>3</sup>

In this report, we detail the methodology behind the proposed architecture, including the integration of SSI and SBTs, and present the results of our implementation. We demonstrate how this approach mitigates the risks associated with centralized authentication servers and improves

the overall efficiency and security of the healthcare data management system. Finally, we discuss the potential implications of this architecture for the broader healthcare industry and suggest avenues for future research.

## Background

In the field of digital credentials management, the integration of blockchain technology and cryptographic protocols has led to significant advancements. A prominent development is the use of SBTs for issuing and managing digital access credentials.

This section examines various contemporary approaches and innovations in this domain, highlighting the strengths and limitations of each, with a particular focus on privacy, non-repudiation, and regulatory compliance.

The digital credentials management system proposed in Ref. 4 introduces an innovative approach by leveraging an enhanced version of SBTs, referred to as rejectable soulbound tokens (RejSBTs). This system enhances traditional credential features by embedding terms and conditions during issuance and ensuring non-repudiation of reception upon acceptance by users. The RejSBTs guarantee non-repudiation of reception and origin proofs, a critical aspect for legal and security purposes. However, the current protocol lacks encryption measures, as it primarily handles non-sensitive digital access credentials. It is crucial that future integrations align with GDPR regulations to address potential privacy concerns.

Another notable approach is the integration of decentralized identifiers (DIDs) with SBTs in digital authentication systems, particularly in the Web3 and metaverse environments. This scheme proposed by Kim and Ryou (2023)<sup>5</sup> utilizes DIDs for user verification via smart contracts and issues SBTs for seamless integration. To enhance privacy, verification authorities' service providers use zero-knowledge proof (ZKP) systems, ensuring that critical user information remains undisclosed during the verification process. This method increases user convenience by allowing the generation of cryptographic proofs without direct user involvement. Additionally, a unified wallet manages both DID credentials and SBTs, simplifying credential management.

In the context of privacy-preserving credential systems, the use of SBTs combined with selective disclosure mechanisms is gaining traction. One framework<sup>6</sup> proposes issuing credentials as NFTs stored on the Interplanetary File System (IPFS) in an encrypted format. Although this system empowers users with complete control over their credential information, the verification process does not employ ZKPs, potentially limiting its privacy assurances.

An advanced method for private identity verification<sup>7</sup> involves zero-knowledge SBTs, which combine SBTs with ZKPs. This protocol uses the identity holder's private/

public key to encrypt data stored in an SBT. A ZKP is then used for verification, ensuring that the data have not been altered, and that the identity holder meets specific requirements without revealing any personal information. This approach effectively balances privacy and security, making it a robust solution for identity verification.

The metaverse presents unique challenges and opportunities for digital identity management. One implementation<sup>8</sup> focuses on providing age-restricted access in Decentraland (a 3D virtual world browser-based platform) using Ethereum smart contracts and ZKPs. This method allows users to prove their eligibility for certain activities, such as accessing a virtual cinema, without disclosing their real identities. It leverages existing legal frameworks like eIDAS (electronic identification) and W3C Verifiable Credentials, demonstrating the practical application of blockchain technology in maintaining privacy while ensuring compliance with legal standards.

A practical use case for SBTs is the certification of COVID-19 vaccinations. This proposed system<sup>9</sup> employs a decentralized application, where SBTs are issued as non-transferable and revocable tokens, ensuring they align with the non-transferable nature of vaccination records. While this approach addresses the administrative aspects of vaccination certification, it does not explicitly tackle privacy and confidentiality, highlighting an area for future improvement.

Furthermore, the concept of data decentralization extends beyond credential management, offering broader applications across various sectors. One significant challenge, aside from security, is the storage of large files on the blockchain network, as traditional blockchains lack the capacity to store extensive files like medical images. Integrating decentralized storage solutions such as an IPFS and Solid Pods (personal data stores that provide a place to access, update, and share data) can revolutionize data management and sharing across networks. For instance, IPFS provides a peer-to-peer network for storing and sharing data in a distributed file system, enhancing data availability and mitigating the risk of central points of failure. A security model proposed for data store on IPFS<sup>10</sup> utilizes Shamir's Secret Sharing (SSS) to encrypt data before storage, implemented in Ethereum and operating on a Proof of Work consensus algorithm, necessitating high computational power.

Another challenge with IPFS is that it only provides a hash of the data, complicating the search for related patient records. To resolve this, an Interplanetary Name System-based blockchain has been proposed in Ref. 11, which facilitates data searching by providing a name instead of a hash, thus reducing search time. Blockchain systems are thus used for storing, sharing, using, and manipulating patient data. Another solution is to use Solid pods to store healthcare data. Examples of

**Table 1.** Comparative analysis of credential management solutions

Source	Key Features	Strengths	Limitations	Privacy	Non-Repudiation	Regulatory Compliance
Pericàs-Gornals et al. (2024) <sup>4</sup>	Enhanced SBTs with T&C, ensures non-repudiation of reception	Legal and security assurance, non-repudiation of reception and origin	Lacks encryption measures, primarily for non-sensitive credentials	Low	High	Needs future GDPR alignment
Kim et al. (2023) <sup>5</sup>	DIDs for user verification, ZKP for privacy, unified wallet	Enhanced privacy with ZKP, seamless integration	Complexity of implementation	High	Medium	Aligned with legal standards
Reddy and Kushwaha (2023) <sup>6</sup>	NFTs stored on IPFS, encrypted format	User control over credential information	Lack of ZKP, limited privacy assurances	Low	Medium	Privacy enhancements needed
Cabot-Nadal et al. (2023) <sup>7</sup>	Combines SBTs with ZKP, uses private/public key for encryption	Balances privacy and security effectively	High complexity	High	High	Strong alignment with privacy regulations
Zichichi et al. (2023) <sup>8</sup>	Ethereum smart contracts, ZKPs, eIDAS, W3C VCs	Practical application in metaverse, maintains privacy and compliance	Specific to age-restricted access	High	Medium	Strong compliance with legal standards
Lunesu et al. (2023) <sup>9</sup>	SBTs as non-transferable and revocable tokens	Addresses administrative aspects	Lacks focus on privacy and confidentiality	Low	Medium	Needs enhancements for privacy
Naz et al. (2019) <sup>10</sup>	IPFS for storage, SSS for encryption, PoW consensus	Enhanced data availability, mitigates central points of failure	High computational power, search difficulties	High	Medium	Strong potential but needs optimization for healthcare
Saharan and Prasad (2020) <sup>11</sup>	Facilitates data searching with names instead of hashes	Reduces search time, enhances data sharing and usage	Implementation complexity	Medium	Medium	Strong alignment with data management standards
Prop.	Decentralized authentication with SBTs, private blockchain (Hyperledger Besu), PoA consensus (QBFT), privacy-aware oracles (Chainlink)	Comprehensive framework, scalable, enhanced security with private smart contracts	Private Blockchain	High	High	Strong compliance focus, private blockchain ensures privacy

DID: decentralized identifiers; eIDAS: electronic Identification, Authentication and Trust Services; GDPR: General Data Protection Regulation; IPFS: InterPlanetary File System; NFTs: non-fungible tokens; PoA: Proof of Authority; PoW: proof of work; QBFT: Quorum Byzantine Fault Tolerant; SBTs: soulbound tokens; SSI: Self-Sovereign Identity; SSS: Shamir's Secret Sharing; T&C: terms and conditions; VCs: verifiable credentials W3C: World Wide Web Consortium; ZKP: zero-knowledge proof.

their use and techniques to optimize a search have been published.<sup>12,13</sup>

Based on Table 1, our solution outperforms existing methods by offering a comprehensive and scalable framework that balances privacy, security, and regulatory compliance. It uses decentralized authentication with SBTs, a private blockchain, and privacy-aware oracles, ensuring high privacy and strong security. Unlike other approaches, it addresses key limitations such as lack of encryption, complexity, and application constraints, making it a superior and more robust option.

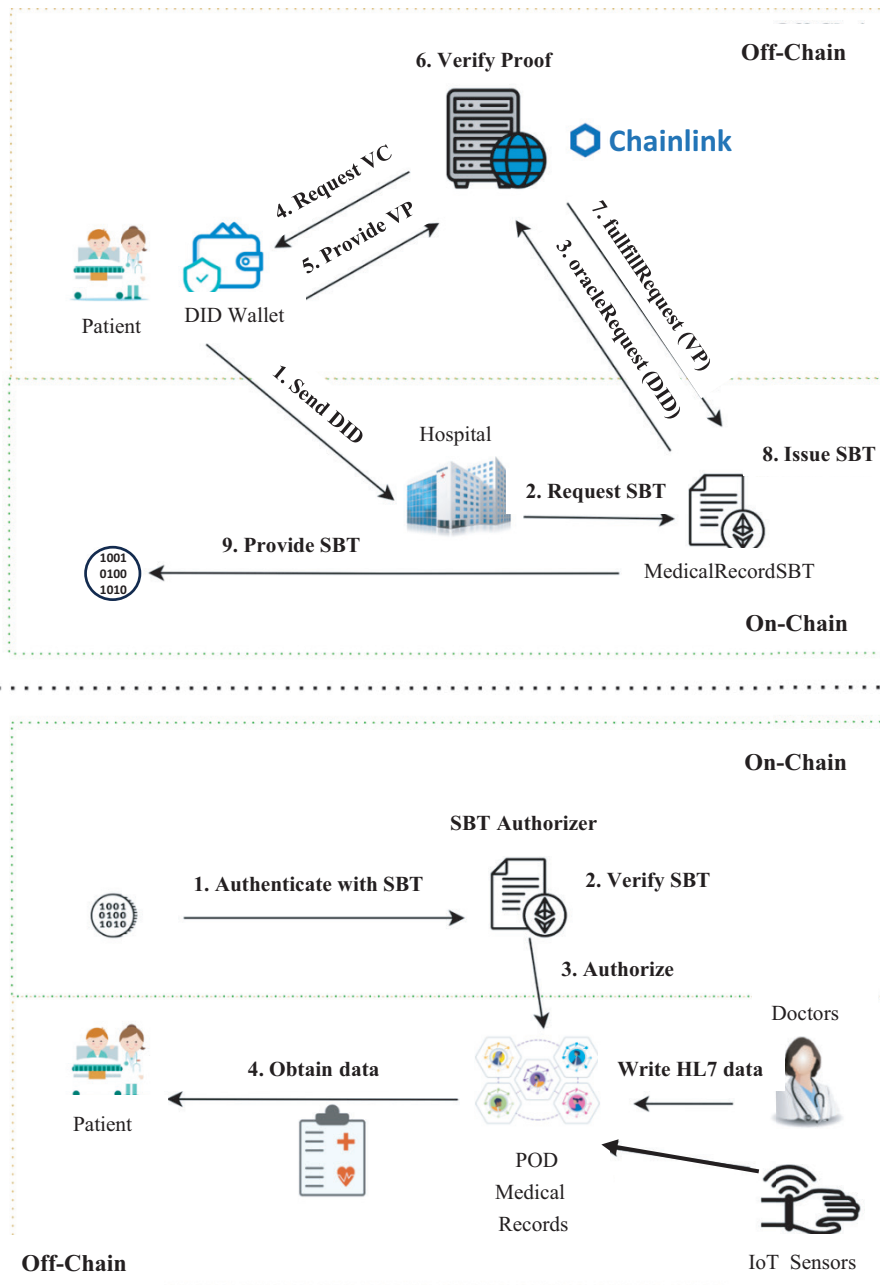
### Proposed System

The advancements in digital credentials management systems using SBTs illustrate significant progress in enhancing privacy, security, and user convenience. However, each approach has its set of strengths and limitations, particularly concerning privacy preservation

and regulatory compliance. Future developments must focus on integrating robust encryption measures, comprehensive privacy protections, and adherence to regulatory standards to fully realize the potential of these innovative systems in digital credential management.

The current state-of-the-art highlights a significant lack of interoperability among data generated within the healthcare domain. By leveraging standards such as HL7, it is feasible to develop interoperable solutions across different hospitals. However, the existing data storage methods, which predominantly rely on centralized servers, require careful redesign. This includes revisiting the mechanisms provided for data access.

The proposed architecture aims to deliver a comprehensive framework for managing authentication in a decentralized manner while also considering the decentralized data solutions discussed in the preceding section.



*Fig. 1.* System Model: enrollment phase (top figure) and authentication (bottom figure). HL7: Health Level Seven; IoT: internet of things; Pods: personal online data stores; SBT: soulbound token.

The objective is to validate this approach by providing insights into the mean response time and a thorough security assessment of the protocol.

### Introduction

The use of DID is not a directly applicable choice in the medical domain due to complex interaction. Moreover, authenticating with SSI poses significant challenges within decentralized applications due to the requirement for signature verification on the credentials, which cannot be performed on-chain without revealing user data.

These concerns become more critical when using public blockchains such as Ethereum.

Our architecture aims to provide all the advantages of SSI while incorporating a novel authentication mechanism based on NFTs, specifically an extension known as Soulbound Tokens (SBTs). SBTs are designed to bind tokens to their owner, thereby leveraging the benefits introduced by NFTs.

To analyze our system, we divide it into two main phases: the enrollment phase, depicted at the top of Figure 1, and the authentication phase, shown at the

bottom of Figure 1. Before going deeper into analyzing these phases, it is necessary to clarify some technical aspects related to our architecture.

Credential verification is complex to on-chain; for this reason, we adopted a hybrid approach, where identity is verified off-chain, and then an SBT is released using a private blockchain, such as Hyperledger Besu. Needs for a private blockchain come from the need to guarantee a user's privacy when performing on-chain transactions.

### Quorum and Proof of Authority

The architecture has been deployed on a private blockchain using Hyperledger Besu, composed of four nodes as part of an experimental project. This setup is easily scalable because we only use blockchain to release SBT. In the employed Proof of Authority (PoA) consensus mechanism, the validators, which are nodes authorized to mine blocks, are pre-authorized by the blockchain owner.

Each block is validated by one of these pre-authorized nodes. Hyperledger Besu supports various PoA schemas, including QBFT, IBFT 2.0 (Istanbul Byzantine Fault Tolerance), and Clique. For the purposes of our project, we selected QBFT due to its ability to ensure the privacy of transactions, which is essential for implementing a privacy-aware oracle based on Chainlink infrastructure. These transactions are secured and accessible only to the parties involved. The scalability of PoA is advantageous, as it supports network growth without significant performance issues. Security and trust are enhanced because validators are trusted entities, reducing the risk of malicious activity and ensuring credible issuance of SBTs. We selected the QBFT schema within PoA for its transaction privacy features, crucial for our privacy-aware oracle using Chainlink infrastructure. Overall, PoA's efficiency, scalability, security, and privacy make it an ideal choice for our SBT deployment.

### Enrollment

The need for an enrollment phase arises from the complexity of creating a timely procedure for authenticating users within the system. Authentication based on DIDs requires verification of credentials and the generation of verifiable proofs by the holder, which can introduce overhead. Additionally, these processes cannot be applied to a public blockchain as previously described.

In our proposal, the first phase involves nine steps to deliver an SBT to the user. During this phase, the user shares the SSI credentials and receives an SBT. The procedure begins with the holder requesting an SBT release from the hospital. During this request, the holder communicates their  $DID_H$ , which, in our case, is a *did:eth* (decentralized identifier:Ethereum) method identifier, to ensure compatibility with the Ethereum blockchain. Such  $DID_H$  is associated with a  $DIDDocument_H$  through the use of

the smart contract previously registered. The hospital forwards the request to the MedicalRecordSBT smart contract containing the same  $DID_H$ , previously deployed on the Besu blockchain. The function requestSBT then forwards this request to the Chainlink infrastructure, which handles off-chain communication with the external server.

As illustrated in Figure 1, during steps 4, 5, and 6, the requests follow the classical SSI trust triangle approach, where the verifier, which, in this case, is the ChainLink node, sends a request to the off-chain server, which generates a VPR. The users generate a verifiable presentation connected to that VPR and transmits it to the off-chain server, which performs credential verification. Once the validity of the transmitted credentials is confirmed, a callback is executed on the MedicalRecordSBT, releasing the final SBT to the user. This SBT can now be used by the user to authenticate themselves on hospital-trusted platforms.

### Authentication

At the beginning of the authentication, the patient already possesses an SBT representing their identity within the hospital. This token is used to authenticate the user and access personal data stored on the POD. The entire procedure is managed through the *SBTAuthorizer* smart contract, which contains references to the issued SBT and is capable of performing the authentication process. This smart contract also includes metadata related to revoked tokens and roles within the system, allowing the hospital to revoke access if a user loses ownership of their wallet.

Similarly to the patients, the internet of things (IoT) devices and the doctors will access the data spaces by using a decentralized approach. As described in Ref. 14 and in Ref. 15, both doctors and IoT device can implement this kind of authentication using SSI. In particular, the doctors will manage authentication through the use of the HSM as a mechanism for reducing time needed for authentication, while IoT devices can leverage physical characteristics, such as Static Random Access Memory (SRAM), or electrocardiogram in order to create a private key used in the SSI wallet generation. Finally, the proposed architecture separates the authentication process from data storage.

### Decentralized Data Storage

The proposed approach also includes a novel decentralized data storage system, which is fully compatible with the proposed decentralized authentication mechanism. Solid, a relatively new framework, aligns with the user-centric data storage paradigm by empowering users to take responsibility for the data produced by applications. In this specific use case, this pertains to the medical data generated by both IoT devices and analyses conducted by doctors. Solid offers a well-structured method for storing data, utilizing knowledge graph technology.

**Table 2.** Costs for the deployment of the proposed architecture

Operation	Gas Needed	Cost (\$)	Spent by
<b>Deployment</b>			
• TokenLink.(constructor)	1467527 gas	11.87	Authority
• Operator.(constructor)	4184013 gas	33.83	Authority
• EthereumDIDRegistry.(constructor)	574518 gas	1.55	Authority
• NationalHealthServiceDIDRegistry.(constructor)	1168361 gas	9.45	Authority
• MedicalRecordSBT.(constructor)	5159457 gas	41.72	Authority
<b>Enrollment</b>			
• EthereumDIDRegistry.updateDIDDocument(string,bytes)	742188 gas	6.00	Hospital
• NationalHealthServiceDIDRegistry.authorizeDID(string,string)	58569 gas	0.47	Hospital
• MedicalRecordSBT.requestSBT(string)	164520 gas	1.33	Hospital
<b>SBT Minting</b>			
• MedicalRecordSBT.fulfillRequest(string)	2594670 gas	20.98	Chainlink Node

DID: decentralized identifiers/identity; SBT: Soulbound Token.

This representation is fully compliant with contemporary data representation mechanisms in the medical domain, such as HL7, which provides a well-documented ontology. This approach enhances the compliancy with respect to GDPR by promoting decentralized data storage, where users can manage data produced by IoT devices, without any copy on external servers.

## Results

To evaluate the quality of the proposed architecture, we mainly focus on the cost for the deployment of the solution in terms of fee for the execution of a smart contract. For the evaluation of our proposal, we deployed a Hyperledger Besu Docker image equipped with QBFT consensus over an iMac 3.3 GHz Intel Core i5 6 cores equipped with 16 GB 2667 MHz DDR4.

To implement our solutions, we deployed five smart contracts:

1. **LinkToken.sol:** Responsible for the payment of Chainlink requests. Initially deployed with 1.000.000 LINK.
2. **Operator.sol:** Responsible for operating with the Chainlink node, which forwards all the requests.
3. **EthereumDIDRegistry.sol:** Responsible for managing the DIDs architecture.
4. **NationalHealthServiceDIDRegistry.sol:** Responsible for managing the roles within the entire framework.
5. **MedicalRecordSBT.sol:** Containing the SBT definition and operation for minting the SBT.

As reported in Table 2, the smart contract deployment is the most expensive operation, together with SBT minting, needed to generate and release the SBT to the user. Operational requests are required to setup the entire environment and refer to the mapping of created DID to

the internal registry containing the roles. The gas estimation offers insights about the complexity of the operations involved by the smart contract, but the costs will depend by multiple factors such as occupancy of the network, fee required. By assuming a cost of 3 gwei per gas needed, which is in-line with normal cost of Ethereum blockchain, it is possible to make an estimation over the total cost of the different operations.

The deployment phase is executed only once at the adoption of the system while enrollment and SBT Minting operations are executed for each new patient belonging to the system. A total cost below \$30 per new user in the system is reasonable for the advantages introduced by the proposed approach.

No cost is provided for the authentication procedure, which only consists of reading data from the blockchain, without requesting any additional fee.

The overall time for the enrollment procedure is about 16.03 s on average; the greatest part is spent verifying credentials (12.54 s). That is the main motivation that led us to move to a fully decentralized and on-chain approach. With our proposal, it is possible to authenticate now using the SBT and by only checking the presence of the SBT on the MedicalRecordSBT smart contract.

With the current research, we tried to reduce the overall time needed for authentication by providing an on-chain verification method while preserving the privacy of nodes and all the advantages introduced by SSI. The overhead introduced by the proposed architecture is relatively low, considering that the enrollment phase is executed only once for each user, and the authentication phase is reduced to a single call to the smart contract. Moreover, the system is strictly based on the blockchain and on the asymmetric mechanism behind the blockchain. SBTs increase security by leveraging a cryptographic wallet, which stores the private key associated with the public one.

## Conclusion

In the future, we plan to enhance our evaluation of the proposed methods by integrating provider access into real-world scenarios. By incorporating provider access, we will be able to simulate more complex, multi-stakeholder environments, which will offer a more comprehensive assessment of our approach's effectiveness in practice. This will allow us to better understand the real-world impact on medical data security and privacy. For example, in a diabetes use case, provider access would enable healthcare professionals to interact directly with patient data stored in Solid Pods while also contributing to and benefiting from a distributed machine learning model. This added layer of provider interaction is essential for validating the scalability and practicality of our architecture across various medical use cases.

## Funding

This work was partially supported by project SERICS (PE00000014) under the NRRP MUR program funded by the EU—NGEU and by the project “DHEAL—COM-Digital Health Solutions in Community Medicine” under the Innovative Health Ecosystem (PNC)—National Recovery and Resilience Plan (NRRP) program funded by the Italian Ministry of Health.

## Conflicts of Interest

None reported by the authors.

## Contributors

Mr. Boi contributed to the conceptualization of the system, the evaluation of the system, and the writing. Mr. Cirillo contributed to the conceptualization of the system, the state of the art, and the overall writing of the paper. Mr. De Santis contributed to the conceptualization of the system and the writing of the paper. Dr. Esposito contributed to the conceptualization of the system and the review of each draft.

All authors have approved the manuscript and agree with its submission to *Blockchain in Healthcare Today*.

## Data Availability Statement (DAS), Data Sharing, Reproducibility, and Data Repositories.

Contact the author.

## Application of Generated Text or Related Technology

Artificial intelligence and related technologies were not used in the preparation of this article.

## Acknowledgments

This work was partially supported by project SERICS (PE00000014) under the NRRP MUR program funded

by the EU—NGEU and by the project “DHEAL—COM-Digital Health Solutions in Community Medicine” under the Innovative Health Ecosystem (PNC)—National Recovery and Resilience Plan (NRRP) program funded by the Italian Ministry of Health.

## References

1. Reegu F, Abas H, Jabbari A, Akmam R, Uddin M, Wu CM, Chen CL, Khalaf O. Interoperability Requirements for Blockchain-Enabled Electronic Health Records in Healthcare: A Systematic Review and Open Research Challenges. *Security and Communication Networks* 2022; 2022(1):9227343. <https://doi.org/10.1155/2022/9227343>
2. Gupta D, Mazumdar N, Nag A, Singh J. Secure data authentication and access control protocol for industrial healthcare system. *Journal of Ambient Intelligence and Humanized Computing* 2023; 14(5):4853–4864. <https://doi.org/10.1007/s12652-022-04370-2>
3. Esposito C, Horne R, Robaldo L, Buelens B, Goesaert E. Assessing the solid protocol in relation to security and privacy obligations. *Information* 2023; 14(7):411. <https://doi.org/10.3390/info14070411>
4. Pericàs-Gornals R, Mut-Puigserver M, Payeras-Capellà MM, Cabot-Nadal MÀ, Ramis-Bibiloni J. Digital credentials management system using rejectable soulbound tokens. *Ann Telecommun [Internet]*. 2024 Apr 23 [cited 2024 Jun 19]; Available from: <https://link.springer.com/10.1007/s12243-024-01032-6>
5. Kim G, Ryou J. Digital Authentication System in Avatar Using DID and SBT. *Mathematics*. 2023 Oct 22;11(20):4387. <https://doi.org/10.3390/math11204387>
6. Reddy S, Kushwaha DS. Framework for privacy preserving credential issuance and verification system using soulbound token. Sumathi AC, Yuvaraj N, Ghazali NH, editors. *ITM Web Conf*. 2023;56:06002.
7. Cabot-Nadal MÀ, Playford B, Payeras-Capellà MM, Gerske S, Mut-Puigserver M, Pericàs-Gornals R. Private Identity-Related Attribute Verification Protocol Using SoulBound Tokens and Zero-Knowledge Proofs. In: 2023 7th Cyber Security in Networking Conference (CSNet) [Internet]. Montreal, QC, Canada: IEEE; 2023 [cited 2024 Jun 19]. p. 153–6. Available from: <https://ieeexplore.ieee.org/document/10339754/>
8. Zichichi M, Bomprezzi C, Sorrentino G, Palmirani M. Protecting digital identity in the Metaverse: the case of access to a cinema in Decentraland. In: International conference on developments in language theory. 2023. Available from: [https://ceur-ws.org/Vol-3460/papers/DLT\\_2023\\_paper\\_13.pdf](https://ceur-ws.org/Vol-3460/papers/DLT_2023_paper_13.pdf)
9. Lunesu MI, Tonelli R, Pinna A, Sansoni S. Soulbound Token for Covid-19 Vaccination Certification. In: 2023 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops) [Internet]. Atlanta, GA, USA: IEEE; 2023 [cited 2024 Jun 19]. p.
10. Naz M, Al-zahrani FA, Khalid R, Javaid N, Qamar AM, Afzal MK, et al. A Secure Data Sharing Platform Using Blockchain and Interplanetary File System. *Sustainability*. 2019 10;11(24):7054. <https://doi.org/10.3390/su11247054>
11. Saharan R, Prasad R. Blockchain Technology for Healthcare Data. *Advances in intelligent systems and computing*. 2020 2;671–7. [https://doi.org/10.1007/978-981-15-6014-9\\_81](https://doi.org/10.1007/978-981-15-6014-9_81)
12. Ghayvat H, Zuhair M, Shukla N, Kumar N. Healthcare-CT: Solid PoD and Blockchain-Enabled Cyber Twin Approach



for Healthcare 5.0 Ecosystems. IEEE internet of things journal. 2024 Feb 15;11(4):6119–30. <https://doi.org/10.1109/JIOT.2023.3312448>

13. Ragab M, Savateev Y, Oliver H, Tiropanis T, Poulouvassilis A, Chapman A, et al. Unlocking the Potential of Health Data with Decentralised Search in Personal Health Datastores. 2024 May 13.
14. Barbareschi M, Boi B, Cirillo F, De Santis M, Esposito C. CSecuring the Internet of Medical Things using PUF-based SSI Authentication. In Proceedings of the 8th Italian Conference on Cyber Security (ITASEC 2024) 2024.
15. Boi B, Esposito C. Securing the Internet of Medical Things with ECG-based PUF encryption. IET Cyber-Physical Systems: Theory & Applications 2024.

### Appendix: Acronyms Defined

DID: decentralized identifiers/identity

did:eth: decentralized identifier:Etherium

DIDDocument<sub>H</sub>: digital identity document (holder)

DID<sub>H</sub>: digital identity (holder)

eIDAS: electronic Identification, Authentication and Trust Services.

GDPR: General Data Protection Regulation

HIPAA: Health Insurance Portability and Accountability Act

HL7: Health Level Seven

HSM: hardware security module

IBFT: Istanbul Byzantine Fault Tolerance

IoT: internet of things

IPFS: InterPlanetary File System

NFT: non-fungible token

PoA: proof of authority;

Pod: personal online data store

PoW: proof of work

QBFT: Quorum Byzantine Fault Tolerant

RejSBTs: rejectable soulbound tokens

SBT: soulbound token

SRAM: Static Random Access Memory

SSI: self-sovereign identity

SSS: Shamir's Secret Sharing

T&C: terms and conditions

VCs: verifiable credentials

VPR: verifiable presentation request

W3C: World Wide Web Consortium

ZKP: zero-knowledge proof

**Copyright Ownership:** This is an open-access article distributed in accordance with the Creative Commons Attribution Non-Commercial (CC BY-NC 4.0) license, which permits others to distribute, adapt, enhance this work non-commercially, and license their derivative works on different terms, provided the original work is properly cited, and the use is non-commercial. See: <http://creativecommons.org/licenses/by-nc/4.0>