TU Delft

Delft University of Technology

Decentralized security in blockchain-based digital health systems

Self-sovereign identity, access control, and auditing with smart contracts

de R. dos Santos, Yago; de Oliveira, Nicollas R.; Barbosa, Guilherme N.N.; Reis, Lucio Henrik A.; Mendes, Ana Carolina R.; de Oliveira, Marcela T.; de Medeiros, Dianne S.V.; Mattos, Diogo M.F.

DOI
10.1007/s10586-025-05669-3

Publication date
2025

Document Version
Final published version

Published in
Cluster Computing

Citation (APA)
de R. dos Santos, Y., de Oliveira, N. R., Barbosa, G. N. N., Reis, L. H. A., Mendes, A. C. R., de Oliveira, M. T., de Medeiros, D. S. V., & Mattos, D. M. F. (2025). Decentralized security in blockchain-based digital health systems: Self-sovereign identity, access control, and auditing with smart contracts. *Cluster Computing*, *28*(15), Article 940. https://doi.org/10.1007/s10586-025-05669-3

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

Green Open Access added to TU Delft Institutional Repository
as part of the Taverne amendment.

More information about this copyright law amendment
can be found at https://www.openaccess.nl.

Otherwise as indicated in the copyright section:
the publisher is the copyright holder of this work and the
author uses the Dutch legislation to make this work public.

Cluster Computing (2025) 28:940
https://doi.org/10.1007/s10586-025-05669-3

Decentralized security in blockchain-based digital health systems: self-sovereign identity, access control, and auditing with smart contracts

Yago de R. dos Santos[1] · Nicollas R. de Oliveira[1] · Guilherme N. N. Barbosa[1] · Lucio Henrik A. Reis[1] · Ana Carolina R. Mendes[1] · Marcela T. de Oliveira[2] · Dianne S. V. de Medeiros[1] · Diogo M. F. Mattos[1]

Received: 1 May 2025 / Revised: 14 July 2025 / Accepted: 29 July 2025
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2025

Abstract
The expansion of Digital Health brings increasing data privacy and security challenges, mainly due to data collection by service providers and third parties. The decentralized approach of Self-Sovereign Identity emerges as a solution, offering users direct control over their data. This paper proposes the SmartMed system for controlling access to private medical data by attribute-based access control implemented on smart contracts. The paper investigates the performance limitations of the Ethereum, Besu, and Hyperledger Fabric blockchain platforms in controlling access to medical data. The proposal develops smart contracts to perform attribute-based access control and to store log records on the blockchain, highlighting the detailed performance analysis on both tested platforms. The results reveal the superiority of the Hyperledger Fabric platform over Ethereum and Besu, indicating a higher transaction throughput. Our proposal innovates by proposing a system based on smart contracts to guarantee the authenticity of medical data, complemented by the use of Keycloak in managing access to healthcare systems.

Keywords Self-sovereign identity · Access control mechanism · Smart contracts

1 Introduction

The global telemedicine market has shown accelerated growth, estimated at a Compound Annual Growth Rate (CAGR) of 17.96% between 2024 and 2030, driven by factors such as greater patient acceptance, digitalization of healthcare services, and strategic investments by large companies in the sector[1]. In Brazil, digital health has also experienced remarkable growth. In 2023, more than 1,400 municipalities embraced telemedicine initiatives, resulting in over 950,000 telehealth diagnostics conducted. Additionally, there was a notable surge in the volume of examinations documented in the National Health Data Network (*Rede Nacional de Dados em Saúde* - RNDS), with a record-breaking 70 million exams conducted that year[2]. Segments such as teleradiology, telepsychiatry, and telemonitoring services have stood out, while integration with mobile and web platforms has consolidated itself as the main delivery model. However, as the Internet landscape evolves towards Web 3.0, privacy and data security concerns become more pressing, especially regarding the collection and exploitation of user data by various entities, including Internet Service Providers (ISPs) and third-party platforms [1]. The lack of transparency in data handling practices and the potential for exploitation without user consent highlight the need for robust identity management structures. In response to these challenges, decentralized technologies such as blockchain offer promising solutions, providing secure and transparent storage and transaction mechanisms. However, the specific application of these technologies in the healthcare sector introduces additional complexities, especially in defining and managing distributed identities in federated health data spaces [2].

[1] Available at https://www.grandviewresearch.com/industry-analysis/telemedicine-industry.

[2] Available at https://www.gov.br/saude/pt-br/assuntos/balanco-2023.

✉ Nicollas R. de Oliveira
nicollas_rodrigues@id.uff.br

[1] LabGen/MídiaCom – PPGEET/TET/TCC, Universidade Federal Flumimense (UFF), Niterói, Rio de Janeiro, Brazil

[2] Delft University of Technology (TU Delft), Delft, The Netherlands

Published online: 09 October 2025

Traditional healthcare identity systems are typically centralized and owned by Identity Providers. As such, creating redundant patient identities in different systems is common, making data consolidation and interoperability difficult. The emergence of Self-Sovereign Identity (SSI) through decentralized technologies presents a paradigm shift, empowering individuals with complete control over their personal data and enabling selective sharing. SSI offers a secure and decentralized approach to identity verification and authorization in healthcare, granting patients and providers direct authority over identity claims. Leveraging blockchain, SSI ensures secure storage and management of data, preserving patient privacy and enabling secure data sharing among authorized parties. However, challenges persist in integrating SSI into existing healthcare systems and ensuring compliance with privacy regulations, such as the General Data Protection Regulation (GDPR), highlighting the need for innovative and interoperable identity management frameworks tailored to the healthcare domain [3].

This paper proposes the SmartMed system and assesses the implications of using Ethereum, Besu, and Hyperledger Fabric blockchain platforms to control access to medical data. Smart contracts were developed to regulate access and maintain medical systems' access logs on both blockchain platforms. These environments were integrated into the SmartMed system, allowing for a comprehensive evaluation of its performance. The main contribution of this work is a detailed analysis of the performance of the proposed smart contracts on the Ethereum, Besu, and Hyperledger Fabric platforms. To assess these platforms, we developed a minimum viable product of the SmartMed system and integrated it with three blockchain environments. The results demonstrate that the Hyperledger Fabric platform performs better than Ethereum and Besu, with a higher transaction throughput and minimum response time.

This paper extends our previous work [4] by introducing smart contract portability and evaluating the performance of the Hyperledger Fabric platform. Other related works explore the use of blockchain technology in medical applications, focusing on secure sharing of Electronic Medical Records (EMRs). Commercial solutions, such as Medicalchain [5], offer users control over medical data but do not address multi-level access. Academic proposals, such as AuditChain [6], FHIRChain [7], and Ancile [8], implement smart contracts for multi-level control but face challenges such as high costs and complexity. This work proposes a blockchain-based system using smart contracts to ensure the authenticity of medical data, using Keycloak to manage access to healthcare systems.

The paper is structured as follows. Challenges for distributed digital health are addressed in Section 2. Section 2.1 examines the main challenges and opportunities for access control using blockchain. Section 3 presents related works. The proposed solution, including its architecture, is presented in Sect. 4. Section 5 discusses the results. Section 6 highlights the limitations of the proposed solution. Finally, Sect. 7 concludes the paper.

2 Privacy and identification challenges for distributed digital health

Data digitization, especially of personal data, has become one of the key challenges related to security. With the COVID-19 pandemic, there was a need to accelerate the process of digitizing medical data through Electronic Medical Records (EMRs). Various regulations address this topic, such as the General Data Protection Law (*Lei Geral de Proteção de Dados* - LGPD) in Brazil and the General Data Protection Regulation (GDPR) in Europe. These data have distinct characteristics from other personal data, as they are considered sensitive by both regulations. In the United States, there is the Health Insurance Portability and Accountability Act (HIPAA), a specific regulation for health data. HIPAA provides guidelines for the collection, storage, and transmission of Protected Health Information (PHI) through technology but lacks practical details for implementing security measures [9]. In all cases, there is a need to ensure that information is protected from breaches, *i.e.*, not leaked, especially for commercial purposes. Traceability of personal data sharing is an extremely challenging task, as data may circulate through a variety of tools without leaving records, often without the knowledge or consent of the data owner. This indiscriminate flow directly affects individuals' privacy. In this context, laws regulating data protection have become vital to assign responsibilities; however, they lack robust technical mechanisms to ensure their effective enforcement.

Digital health data is stored electronically through Electronic Medical Records (EMRs) and is typically distributed through data silos, resulting in fragmented information [10]. The diversity of records and fragmentation create challenges in processing this data [11], making privacy assurance difficult and practically impossible to detect potential breaches. Alongside privacy concerns, data partitioning can result in duplication and loss events. Additionally, technical and technological challenges exist in controlling access to patient data from remote healthcare units. In some cases, there is an internal culture within healthcare units of improper sharing of access credentials among professionals on the same team, which facilitates the creation of an environment where access logs are unreliable and auditing is complex. Another critical factor is that in many hospitals, access control to patient data is based on Role-Based Access

Control (RBAC) [12], allowing doctors who are not treating a patient to access their medical records, invading their privacy.

In the United States, the Office of the National Coordinator for Health Information Technology (ONC) is the government entity responsible for coordinating efforts to implement and use technologies applied to health data. Guidelines and regulations have been proposed to ensure that access to medical data is controlled, addressing security and privacy issues. Among the regulations, one is responsible for Identity Verification and Authentication, where patient authentication plays a critical role in healthcare institutions, aiming to preserve data and prevent fraud [13]. Using computational technologies to control access to data is essential due to the complex scenario of medical records privacy and increasingly stringent legislative requirements. One of the main challenges faced by healthcare institutions is to ensure that data access is granted only to authorized professionals, based on a certain context. However, the main goal of an EMR system is to provide patient data, and therefore, access control should not prevent legitimate requests in the best interest of the patient [14]. In this sense, the existence of a reliable, auditable, and distributed access control system for data access becomes indispensable. Blockchain technology implements security mechanisms that ensure the immutability, non-repudiation, integrity, and auditability of access to electronic medical records.

In the digital health scenario, identity management assumes an increasingly crucial role. Traditional identity systems, often centralized and controlled by governmental or private entities, present several limitations that raise growing concerns, especially regarding privacy and security in accessing data associated with credentials. Centralized control and lack of interoperability between different identity systems exacerbate these concerns. Self-Sovereign Identity (SSI) emerges as an alternative paradigm, offering individuals unprecedented control over their personal data and unparalleled autonomy in how they share it [15]. SSI differs from traditional identity systems by relying on innovative principles regarding user control, decentralized identity management, and cryptographically verifiable credentials.

The widespread implementation of SSI can bring several benefits, especially to healthcare systems. In the context of digital health, one of the greatest benefits of SSI is placing data control in the hands of individuals, allowing them to decide which information to share and with whom. This protects individual privacy and reduces the risk of identity theft and other forms of fraud [16]. In terms of security, the decentralized nature of SSI makes it more resistant to cyberattacks and identity fraud, protecting valuable information against unauthorized access. Cryptographically verifiable credentials ensure the authenticity and reliability of identities, making it difficult to forge or manipulate data. SSI promotes a safer digital environment for all users [15].

Due to its decentralized nature and greater user control, the implementation of SSI in healthcare systems faces significant challenges [17], which need to be carefully considered to ensure security, privacy, and efficiency. Although the main goal of adopting SSI is to empower patients with full control over their identity information, there are obstacles to overcome. In traditional centralized models, healthcare service providers are responsible for protecting patients' privacy, but this requires complete trust from patients in providers. Additionally, these models can be susceptible to data loss and security breaches. Blockchain-based SSI offers a potential solution, allowing patients to control their information and ensuring its security. However, there are still uncertainties about the precise definition and implementation of SSI, as well as technical challenges in effective implementation, such as decentralized identification and interoperability. To advance the adoption of SSI in the healthcare sector, it is crucial to address these issues and ensure compliance with privacy regulations, such as LGPD in Brazil, GDPR in Europe, and ONC definitions in the United States. To address these limitations, recent research has explored the use of blockchain as a foundational technology to support decentralized identity models, including SSI. By offering tamper-resistant and transparent data management, blockchain can serve not only as a secure registry for identity credentials but also as a reliable mechanism for enforcing access control policies without relying on a central authority. Despite its advantages in terms of privacy and individual control, the SSI model has vulnerabilities that must be considered. The absence of a central authority places greater responsibility on users to manage their private keys, the loss of which can result in complete inaccessibility to their digital identity. Additionally, reliance on personal devices for storage and authentication exposes the system to physical risks and malware attacks. Another significant limitation is the difficulty of efficiently revoking compromised credentials, especially in distributed environments without a central repository. These issues highlight the need for complementary recovery, revocation, and continuous monitoring mechanisms to ensure the security of the SSI ecosystem. To systematically overcome these limitations and fortify the integrity of decentralized identity, blockchain technology emerges as a foundational and indispensable solution. Its tamper-resistant ledger and inherent transparency provide a secure and auditable method for managing identity credentials while enabling the autonomous enforcement of access policies.

2.1 Blockchain for access control

Blockchain technology consists of two elements: a data structure for chaining blocks, and a peer-to-peer (P2P) network capable of storing transactions in an ordered and distributed manner. One of the primary purposes of this technology is to ensure security and resilience in environments where there is no mutual trust between network participants, allowing the removal of the central entity that guarantees trust between parties [18]. Blockchain inherently guarantees the integrity of the stored data, as changing or deleting such data is practically unfeasible. Other blockchain's fundamental properties are transparency and traceability of data. The stored data is accessible to all participants in the peer-to-peer network. Therefore, storing unencrypted sensitive data is not recommended.

Regarding taxonomy, blockchain network can be classified as public or private and permissioned or permissionless. Permissioning defines the roles that nodes can assume in the network. In permissionless networks, all nodes have the same roles and responsibilities. In permissioned networks, nodes can have different roles depending on their identification in the network. The distinction between public and private determines the criteria for node participation in the peer-to-peer network. In a public network, there is no permissioning, and any node can join the network by providing a portion of its computational power. The public network is highly decentralized and presents various security challenges, as malicious nodes may join the network. Because it is public, the failure of any node does not cause problems in block generation. On the other hand, in private blockchain, there is access control to the network, resulting in a more restrictive and controlled network. According to these categories, blockchain-network taxonomy is Public Permissionless Networks, which do not require access control, and all nodes can generate new blocks, requiring more robust consensus mechanisms; Private Permissionless Networks, which have access control, but all nodes perform the same functions; Private Permissioned Networks, which restrict network access, and there are different roles performed by nodes, with mining nodes responsible for generating blocks and participating in consensus.

Blockchain-based solutions have high availability because all nodes participating in the network have the same information, i.e., an identical replica of the blockchain, with no single point of failure. Therefore, other nodes can still access the information if a node becomes unavailable. To ensure that all replicas of the blockchain are identical, validation and consensus mechanisms must be applied [19]. Since the blocks consist of a sequence of transactions to be executed, the nodes must reach consensus, and agreement must be established regarding the transactions inserted into the block and the execution order. The process of validating and ordering transactions into blocks is known as mining, which is the responsibility of mining nodes. The consensus mechanism used in the network establishes rules that ensure the validation and propagation of transactions and blocks, resolving potential conflicts in the data being transmitted. Once consensus is reached, the integrity and immutability of the information are ensured.

Among the main consensus mechanisms used in blockchain networks in the healthcare sector are: Proof-of-Work (PoW), Proof-of-Stake (PoS), and Proof-of-Authority (PoA). PoW is one of the primary consensus algorithms in blockchain [20]. The process concerns a competition among miners that relies on probabilistic logic. Miners attempt to solve complex cryptographic challenges to record selected transactions in blocks added to the blockchain. Solving the challenges requires a brute force approach, requiring the discovery a numeric value known as a cryptographic nonce. The nonce and the selected transactions are incorporated into a candidate block for subsequent validation by the network. This process ensures security, as multiple nodes verify each block before being accepted as part of the blockchain. Unlike PoW, PoS is a consensus mechanism in which the success of mining a block depends on the node's participation in the network. Nodes compete to find the cryptographic summary value lower or equal to a target value, allowing them to mine a new block. However, the difficulty of determining this cryptographic summary value is inversely proportional to the node's accumulated wealth, known as coinage. The accumulated wealth is calculated as the amount of resources the node holds multiplied by the period the node has kept these resources. Thus, the node with the highest accumulated wealth will more likely validate the following blocks. Finally, PoA is a consensus mechanism mainly used in private networks. In this mechanism, a central entity is designated to appoint a specific set of authority nodes. These nodes are responsible for generating new blocks and validating transactions. Including any block in the chain requires validation and signature by at least one authority node. The need for consensus among the authority nodes regarding the global state of the chain ensures the network's decentralization. Some platforms implement a rotating block generation scheme to mitigate conflicts and optimize resource usage, ensuring each authority node has an exclusive time interval to perform this task.

Finally, smart contracts are self-executing applications stored on the blockchain. Initially introduced on the Ethereum platform, smart contracts transform real-world contract clauses into code and are accessible through an address known to all network participants. Within a smart contract reside the rules agreed upon by the parties, which make clause violation computationally prohibitive and not

advantageous for potential malicious parties. Unlike non-deterministic contracts, which face consensus difficulties due to randomness, smart contracts are naturally deterministic [21].

A consortium blockchain, also known as a permissioned blockchain, represents an evolution in the concept of distributed networks, where the control and validation of transactions are restricted to a select group of predefined organizations or companies. In contrast to public blockchains, which work openly and are decentralized, consortium blockchains have controlled participation. As such, consortium blockchains allow only authorized members to contribute to the consensus process and, in many instances, access the stored data. This hybrid approach offers a valuable middle-ground between the relatively low level of trust in public blockchains and the controlled, albeit cryptographically auditable, architecture of private blockchains, which resemble classic centralized systems with a high degree of traceability. In the specific context of consortia, the application of a consortium blockchain offers a range of significant benefits. Enhanced transparency, robust security against fraud and tampering, operational efficiency driven by the automation of processes via smart contracts, complete traceability of operations, and the potential to increase liquidity through the tokenization of quotas are just some of the gains that this technology can provide [22]. The collaboration between trusted organizations within the consortium, comparable to a board of trusted entities, coupled with the ability to control data privacy, makes consortium blockchains a more appropriate choice in scenarios where information protection is crucial, such as in hospitals, contrasting with the objectives of eliminating intermediaries and anonymity of public blockchains.

Hyperledger Fabric establishes itself as an enterprise-grade permissioned blockchain platform under the aegis of the Linux Foundation, meticulously architected to develop distributed solutions and applications that demand strict access control, robust privacy, and optimized performance [23]. Its inherently modular architecture allows for the replacement and customization of crucial components, such as the consensus mechanisms responsible for ordering transactions and the Membership Service Providers (MSPs) managing participant identities. This intrinsic flexibility grants Fabric remarkable adaptability to meet various enterprise use cases' unique and complex requirements, from supply chain tracking to implementing collaborative financial platforms. At the core of Fabric's architecture reside the peers, who act as fundamental nodes in the network and are responsible for hosting full or partial copies of the distributed ledger and executing smart contracts called chaincode. Endorsing peers' primary function is to simulate the execution of proposed transactions and attest to their validity through cryptographic endorsements. Committing peers validate the blocks of transactions sequenced by the ordering service. Together, these peers persist the changes in the ledger, and maintain the integrity of the world state, which represents the current view of assets in the network. The ordering service (orderers) is essential in establishing the canonical order of endorsed transactions, grouping them into blocks, and disseminating them to the committing peers, ensuring transactional consistency across the network. The ledger, in turn, constitutes the immutable and transparent record of all transactions, structured as a chain of cryptographically linked blocks, complemented by the world state, an efficient database for querying the current state of assets. Segregation and access control are refined through channels, which establish private and isolated communication networks between specific subsets of members, each with its own ledger and participating peers, ensuring the confidentiality of the information transacted within this restricted context.

Chaincode, the core logic in Hyperledger Fabric, represents executable programs that interact directly with the ledger. It defines the rules governing the creation, transfer, and modification of assets and the implementation of complex business processes. The lifecycle of chaincode involves installation on the relevant peers, approval by a predefined number of participating organizations in a channel, and finally, the "commit" to make the chaincode operational. The fundamental transaction flow in Hyperledger Fabric (HLF) for recording information on the blockchain comprises three essential steps: endorsement, ordering, and commitment. Initially, in the endorsement phase, the client application submits a transaction proposal to a participating peer in the network and awaits endorsements from endorsing peers [24]. These peers simulate the execution of the chaincode, and if the simulation is successful and meets the defined endorsement policies, a signed response will be returned to the application. The client, aggregating sufficient endorsements, often the majority of participants plus one, submits the transaction to the ordering node, initiating the ordering phase. Network transactions are collected in this phase until the defined batch timeout or batch size parameters are reached to generate a new block. The block size can be defined by size in bytes or by the number of transactions per block, the latter being considered in simplified models. The ordering node sequences the transactions into blocks and distributes them to the committing peers, which perform the final validation before persisting the block in the ledger and updating the world state, notifying the client of the operation's output [23]. A typical and resilient HLF architecture includes two endorsers, an orderer with a Raft consensus mechanism, and two commit nodes, a scalable configuration that allows testing essential functionalities

before larger-scale deployments. It is important to note that endorsers and committers can be the same nodes. In contrast, the ordering node adds validated transactions to a block and distributes it.

The consensus protocol in Hyperledger Fabric is a replaceable component, allowing the adoption of different mechanisms according to the network's specific requirements. Typical implementations include Raft, a leader-based protocol that ensures transaction order and fault tolerance in an environment where a majority of the ordering nodes are trustworthy; Kafka, a high-throughput distributed messaging system that can be used as an ordering service, often combined with an external consensus protocol to ensure total order; Solo, a simplified single-node protocol primarily intended for development and testing environments; and the possibility of integrating Byzantine Fault Tolerance (BFT) protocols for scenarios where resilience to malicious nodes is a primary concern. The choice of consensus protocol directly impacts the network's performance, fault tolerance, and complexity [25]. Granularity in data control is further refined by private data collections, a mechanism that allows restricting access to specific attributes of assets to an authorized subset of organizations within a channel, ensuring an additional level of confidentiality for sensitive information. The versatility and sophistication of Hyperledger Fabric's architecture solidify it as a robust and adaptable platform for building enterprise blockchain solutions that demand a balance between controlled transparency, uncompromising security, and efficient scalability.

3 Related work

The use of blockchain technology in medical applications has gained prominence, especially for its ability to generate irrefutable computational evidence and store it in a distributed manner. This characteristic is particularly valuable in solutions for sharing Electronic Medical Records (EMRs), where traceability of accessed data is crucial. In this context, a wide range of blockchain-based proposals have emerged in both academic literature and the commercial sector, exploring different strategies for managing access, identity, and interoperability in healthcare.

Several commercially available platforms leverage blockchain to enable patient-controlled access to medical data, often relying on token-based mechanisms and permissioned networks. Among these plataforms, Medicalchain [5] uses blockchain to develop medical applications that allow users to control their medical data and choose to share it with qualified professionals. Tokens are used to manage data access. The Medicalchain platform implements two blockchains. The first is used for controlling access to medical data and is built using the Hyperledger Fabric platform. The generation of tokens is the responsibility of the second blockchain. Medicalchain uses the ERC20 (Ethereum Request for Comments 20) of the Ethereum platform for this purpose. The distribution of tokens is controlled by a smart contract stored on the Ethereum blockchain. There is no data storage on the blockchain blocks. This solution does not feature multi-level access.

In parallel, academic research has explored more granular access control schemes, frequently adopting Attribute-Based Access Control (ABAC) models implemented via smart contracts. The AuditChain solution provides multi-level access control for patients, doctors, nurses, and hospital administrators for managing EMRs [6]. The proposal implements smart contracts using the Hyperledger Fabric platform [26, 27]. The digital signature of the transaction uses public key cryptography and serves as a virtual token for access control. However, because it uses the public key, it is subject to high processing costs. AuditChain's evaluation is limited to demonstrating its functional behavior, without performance measurements or systematic security analysis. Zhang *et al.* propose FHIRChain, a blockchain-based architecture that incorporates the HL7 FHIR (Fast Healthcare Interoperability Resources) standard for shared clinical data [7]. Access control is performed through smart contracts on the Ethereum public network, ensuring greater availability. However, the use of the public network implies monetary costs for contract execution. Furthermore, FHIRChain does not include experimental evaluation, neither in terms of performance nor security aspects. Ancile, developed by Dagher *et al.*, is an Ethereum-based blockchain used to manage medical records. It employs smart contracts to control access and protect data, keeping records in the existing databases of providers [8]. While providing a functional demonstration of access control, the proposal does not present performance benchmarks and security evaluation under real-world conditions. SmartAccess framework [10] proposes an Attribute-Based Access Control (ABAC), leveraging XACML primitives, by encapsulating them into smart contracts deployed on a private blockchain. This groundbreaking approach effectively controls access to decentralized medical data, fostering interoperability and ensuring adherence to stringent privacy regulations. Smart contracts ensure security and traceability in transactions accessing confidential data and integrate with electronic medical record systems through the OAuth2.0 protocol. However, SmartAccess focuses solely on controlling access to medical data through a private Ethereum blockchain.

A distinct line of work focuses on decentralized identity management, using blockchain-based Decentralized Identifiers (DIDs) to enhance autonomy, privacy, and interoperability across digital health ecosystems. DID-enabled

systems are designed to provide individuals with full autonomy over their digital identities, removing dependency on centralized authorities. Conventional identity management infrastructures, typically operated by financial institutions or certificate authorities, are susceptible to single points of failure and impose significant limitations on user control regarding data sharing. In contrast, DID-enabled systems use blockchain infrastructure to establish secure, transparent, and user-governed identity management frameworks. The DidTrust protocol, introduced by Yin et al. [28], addresses critical challenges in decentralized identity by incorporating Secure Multiparty Computation (SMPC) to preserve the confidentiality of user feedback and by implementing mechanisms to mitigate trust-related attacks, including Sybil attacks and ballot stuffing. Despite its technical advancements, DidTrust incurs significant computational overhead under high transaction loads, limiting its scalability in heterogeneous environments. Additionally, a comprehensive analysis presented by Mazzocca et al. [29] identifies structural barriers to the widespread adoption of DIDs and Verifiable Credentials (VCs), including interoperability deficiencies, the absence of standardized governance models, and persistent vulnerabilities in key and credential management. Although DIDs and VCs represent a significant theoretical progression in identity decentralization, practical deployments continue to encounter challenges related to scalability, usability, and regulatory compliance. Emerging architectures, such as TDID [30], attempt to mitigate some of these inherent limitations by proposing more efficient data structures and blockchain-integrated identity management. TDID employs Structured Merkle Patricia Trees (SMPT) to improve the performance of identity data retrieval and storage operations, and uses smart contracts to automate identity registration and authentication. Similarly, protocols as SLVC-DIDA [31] propose signature-less VCs to improve privacy and reduce computational burden. However, these newer models introduce additional complexity and rely on cryptographic assumptions that could be challenged in the post-quantum era, highlighting the need for further research on their long-term resilience. In the healthcare domain, several proposals adapt DID frameworks to the particular needs of medical systems. Health-ID [32] implements a blockchain-based decentralized identity management system to allow patients and healthcare providers to authenticate in different eHealth domains. The system uses smart contracts deployed on an Ethereum network consortium and introduces healthIDs attested by regulatory authorities. Although this approach enhances user control over identity attributes, it does not fully address challenges related to dynamic attribute revocation and cross-domain interoperability. Similarly, the proposed decentralized identity system for communities with rare diseases [33] emphasizes user-centric control and interoperability, but remains conceptual, lacking large-scale empirical validation across diverse healthcare providers and regulatory environments. Parallel efforts focus on integrating DIDs into smart healthcare IoT ecosystems. The authentication scheme proposed by Alnour et al. [34] leverages Hyperledger Indy to support decentralized, verifiable interactions between users and medical IoT devices. While this model offers notable improvement over traditional certificate-based authentication, it faces challenges in scalability due to the high latency of blockchain consensus protocols and the operational complexity of managing device-specific DID documents. Furthermore, the dynamic nature of medical IoT systems demands efficient revocation and reissuance mechanisms, which current DID-based approaches only partially address.

Table 1 presents a comparative analysis of existing healthcare blockchain systems and our proposed approach. Furthermore, our approach extends the previous work [4] by introducing three key technical contributions that significantly enhance the SmartMed system.

1. **Triple-Blockchain Evaluation for Access Control**. We conducted a comprehensive triple-blockchain evaluation for access control mechanisms. Beyond the initial assessments with Besu and Ethereum, our current comparison now includes Hyperledger Fabric. This expanded analysis provides critical insights into computational cost and response time variations across these distinct blockchain platforms, highlighting their performance characteristics in a permissioned healthcare context.
2. **Enhanced Smart Contract Portability**. Our second contribution focuses on the significantly enhanced portability of SmartMed's smart contracts. These contracts are now implemented in multiple programming languages and robustly adapted for diverse blockchain

Table 1 Comparative analysis of healthcare blockchain systems

Feature	AuditChain	FHIRChain	Ancile	SmartMed
Access Control	Multi-level RBAC	Smart contracts	Smart contracts	ABAC
Platform	Hyperledger Fabric	Ethereum	Ethereum	Hyperledger Fabric
Identity	Digital signatures	Institutional IDs	Smart contracts	SSI + Keycloak
Consensus	Raft	PoW (Ethash)	PoW (Ethash)	Raft
Interoperability	Limited	HL7 FHIR	API-based	OAuth 2.0
Evaluation scope	Functional only	Conceptual	Functional	Performance only

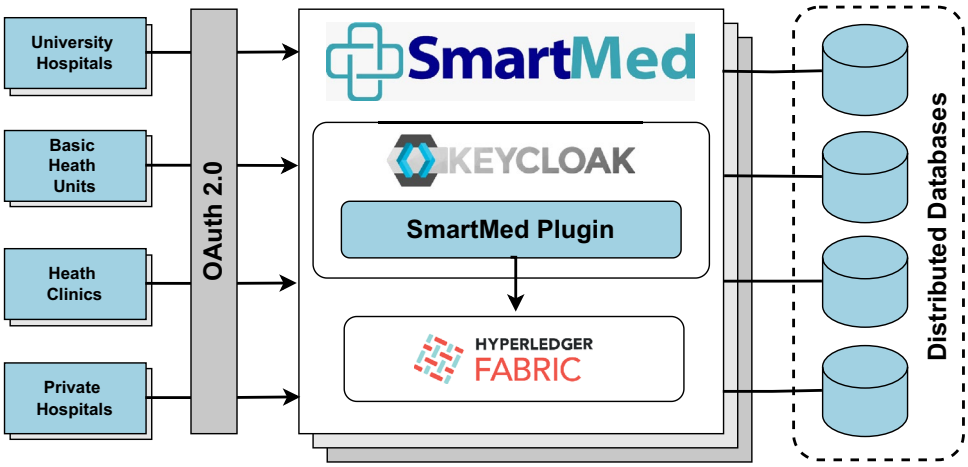


Fig. 1 Proposed architecture for the SmartMed system. Users in healthcare entities request access to distributed databases through OAuth 2.0-enabled applications. The requests are mediated by SmartMed, which determines access authorization based on the outcome of an interaction with the smart contract executing on the Hyperledger Fabric blockchain platforms. All denied and authorized access requests are immutably recorded on the blockchain

platforms. This strategic development substantially augments the system's interoperability and its capacity for seamless integration within heterogeneous healthcare IT ecosystems.

3. **Scalable Containerized Architecture and Deployment**. Finally, we present a refined and expanded system architecture featuring a container-based deployment model leveraging Docker, with advanced orchestration capabilities provided by Kubernetes. This model is engineered to enable the system's efficient execution in highly distributed and scalable environments. Such a design directly addresses and aligns with the stringent operational demands and regulatory requirements of modern healthcare institutions.

4 Proposed architecture for access control and verifiable logs

We propose an architecture for the SmartMed system that aims to address challenges related to the security of EMRs by implementing access control for distributed medical data with refined and robust rules. Figure 1 presents the proposed architecture. Healthcare entities interact with the system through an OAuth 2.0-enabled interface, requesting access to data stored in a distributed database. Healthcare entities are represented by various healthcare software elements that require authentication and access control, such as EMRs or virtual medical appointment tools.

The OAuth 2.0 protocol ensures interoperability between different systems. This protocol allows users to grant a client application the right to access a system or resources from third parties without sharing the user's credentials. Hence, the protocol uses an access token, which represents authorization to access the system or resources on the user's behalf. EMR applications can use the protocol to request access to distributed data.

The proposed system mediates access requests, authorizing or denying access based on the outcome of interactions with a smart contract executing on the blockchain. The system deploys Attribute-Based Access Control (ABAC), which relies on the 5W1H framework (who, what, where, why, when, and how). Access decisions are made by evaluating the attributes associated with the requesting subject, the necessary access level, the desired operation, and any relevant contextual factors related to the request. As the smart contract executes, the request's attributes are assessed, and the system provides an access token that must be used to access the data. Every access request is stored on a blockchain, assembling an auditable and immutable record.

The SmartMed system integrates authentication, authorization, and logging activities with blockchains through a plugin for the Keycloak authenticator[3]. The developed plugin extends Keycloak, an open-source software for identity and access management, enabling interaction with the smart contract stored on the blockchain. The main functionalities of the plugin are (i) forwarding specific log events to the network, (ii) forwarding authorization requests or access control events to a smart contract responsible for evaluating the request, and (iii) receiving and interpreting transaction responses, returning them to Keycloak. It is important to note that SmartMed does not provide identity once it centralizes identity management. Instead, the SmartMed ecosystem consists of paired Keycloak instances and blockchain nodes for each associated organization. For identity governance, SmartMed uses federated identity providers on Keycloak, allowing it to operate independently of a single identity provider.

Implementing the system in university hospitals or other healthcare institutions enables all medical data, whether stored locally or remotely, to be patient-centered and recorded immutably on the network. The proposed system

[3] Available at https://www.keycloak.org/.

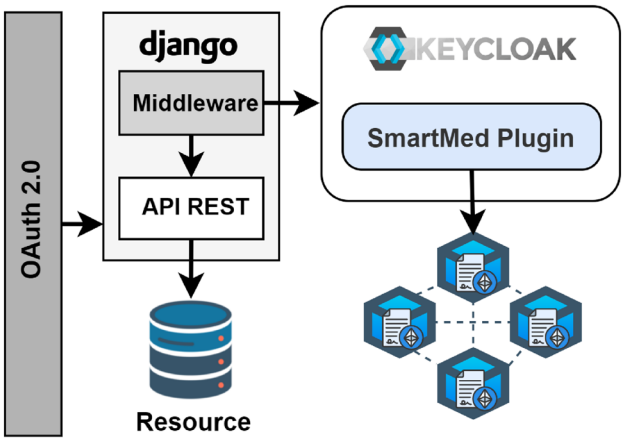


Fig. 2 The proposed system's test environment with a web application based on the Django library. The middleware directs requests to the REST API with user authentication information to Keycloak, which sends them to a smart contract on the blockchain. After evaluation, the middleware grants or denies access to the resource based on Keycloak's response

also enables visual tracking of access request flows through interactive dashboards and allows for the editing of policies tailored to each institution's access profile. Additionally, for simplified deployment, all SmartMed components are delivered in Docker images, conforming to industry best practices. Allowing the configuration of a cluster on Kubernetes or Docker Compose, for instance. Hence, the implementation of the SmartMed ecosystem, which includes Keycloak with the plugin and the Hyperledger Fabric peer node, adheres to a well-established standard.

5 Experimental results

The SmartMed system is implemented as a minimum viable product. To assess the feasibility of this proposed system, three private blockchain networks are created using the Hyperledger Besu, the Ethereum, and the Hyperledger Fabric platforms. The experiments are conducted on a notebook equipped with 16 GB of RAM and an Intel Core i7-10510U processor, running Ubuntu 22.04.4 as the operating system.

The Hyperledger Besu blockchain implements IBFT 2.0 (Istanbul Byzantine Fault Tolerant Protocol 2.0), a Proof-of-Authority (PoA) consensus protocol. Meanwhile, the Ethereum blockchain utilizes the Ethash Proof-of-Work (PoW) algorithm for consensus. Both networks start with the same genesis block and are configured with four interconnected nodes. The Hyperledger Fabric implements the test network on version 2.5 that is available in the official platform repository and documentation[4]. The Hyperledger Fabric test network comprises two organizations' peer nodes, Org1 and Org2, one ordering node utilizing the Raft consensus mechanism, one Certificate Authority (CA) node for each peer, and a single Fabric channel to enable transactions between Org1 and Org2. The networks receive smart contracts from the SmartMed system, which include log registration functionalities and a simple access control policy that verifies if the requester's email address belongs to a pre-established domain. The smart contracts for Hyperledger Besu and Ethereum are written in the Solidity Domain-Specific Language (DSL). For the Hyperledger Fabric, the Go language is used. All relevant codes and configuration requirements are publicly available in the GitHub repository[5].

Figure 2 illustrates the test environment setup. In addition to configuring the blockchain, the proposed system includes a web testing application to evaluate the SmartMed plugin created for Keycloak. This application uses Python 3 and the Django 3.2 library for development. The testing application includes a REST API protected by a middleware executed directly in Django. The middleware intercepts calls to the REST API. It constructs an access request, adhering to Keycloak standards, including the OAuth 2.0 authentication token information, the requested operation scope (read or write), and the desired resource. Hence, the middleware acts as a gateway to the API, known as the Policy Enforcement Point (PEP) in the XACML standard used by Keycloak. The intercepted access requests to resources in the REST API are forwarded to Keycloak for validation. Then, Keycloak forwards the data to the corresponding policy on the blockchain. After evaluation by the policy, the result is returned to the middleware, which grants or denies access to the resource based on Keycloak's response.

The first test focuses on evaluating the performance of the three platforms for executing smart contracts in a permissioned network. The number of Transactions Per Second (TPS) and the gas consumed per relative block are evaluated. The gas consumed per relative block is the ratio of gas accumulated per block to the number of transactions on each block. Using gas consumed per relative block ensures a fair, transaction-level performance comparison between Hyperledger Besu and Ethereum, isolating contract execution cost from unrelated block characteristics such as fullness or consensus behavior. The experiment on Hyperledger Besu and Ethereum directly executes the functions of access policy and logs using JSON-RPC 2.0 calls to the blockchain. For the Hyperledger Fabric, the access to the policies is executed using the Hyperledger Fabric Gateway SDK for Java. Since Hyperledger Fabric focuses on trusted organizational collaboration within a network, it does not utilize the

[4] Available at https://hyperledger-fabric.readthedocs.io/en/release-2.5/test_network.html.

[5] Available at https://github.com/yagorezende/smartmed-mvp.

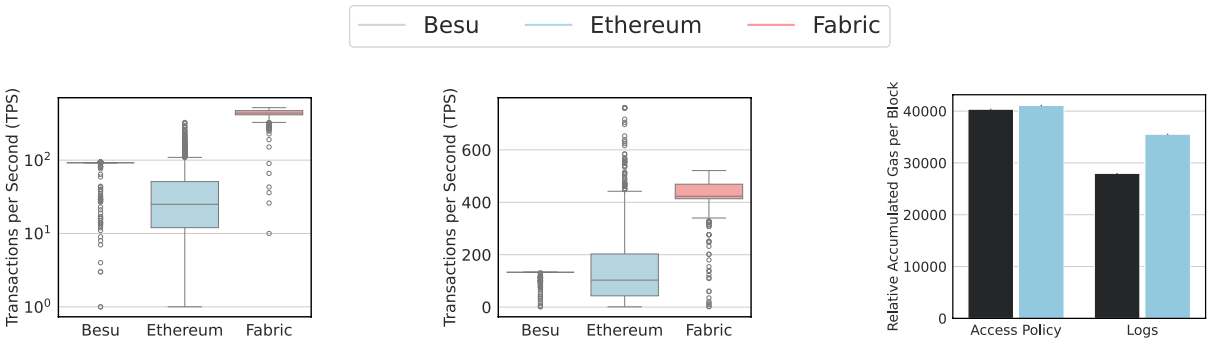
EVM gas fee system. Therefore, gas tests are relevant only for the Hyperledger Besu and Ethereum platforms.

The access policy function is tested using the Faker library for Python 3. It generates 9,000 well-formed email addresses randomly grouped with a thousand instances of the email corresponding to the expected policy domain, increasing disorder and representing a dynamic scenario. For the activity log function, 10,000 random log instances are created following the same logic. Calls to the smart contract functions are executed in bursts of 5,000 sequential requests, and the evaluation code stores all transaction receipts before restarting the test.

The test is repeated 30 times, and the results are presented in Fig. 3 with a 95% confidence interval. For both access control and logging functions, Fig. 3(a) and (b) show that the average number of TPS in the Hyperledger Besu blockchain is higher than in the Ethereum blockchain. Still, Hyperledger Fabric presents almost three times the TPS of the other two platforms. Additionally, the distribution in Hyperledger Besu is the least scattered of all three, indicating a more predictable scenario closer to a constant value. In Fig. 3(c), the gas accumulated per relative block in the access policy function is very close to the gas limit stipulated for the networks, indicating that both Ethereum and Hyperledger Besu platforms have a similar cost for this function. Conversely, the log function shows lower computational cost in Hyperledger Besu.

The second experiment evaluates the performance of the three platforms in the access control of the test application. In this scenario, four access accounts are created in Keycloak to introduce variability in the requests. A thousand sequential requests are sent to the application using the access token of one of the four previously authenticated and randomly selected accounts for each request. The response time of each request is recorded, and the experiment is repeated 30 times. Figure 4 presents the results of the experiment with a 95% confidence interval. Figure 4(a) illustrates the response time for each platform, showing that the implementation based on the Hyperledger Besu platform, which uses the IBFT 2.0 PoA consensus protocol, maintains a stable and approximately constant behavior, with response times of around 2 seconds. On the other hand, the Ethereum-based approach, with the Ethash PoW consensus protocol, exhibits significant variation, with an average of around 10 seconds. Hyperledger Fabric is deployed with the Raft consensus protocol. The average response time for the Hyperledger Fabric is close to 13 ms, more than 100 times less than Hyperledger Besu and almost 1000 times less than Ethereum. In Fig. 4(b), the stable behavior of Hyperledger Besu is again evident, while the Ethereum approach shows significant variation over time, with no indication of stability. For the Hyperledger Fabric, the behavior is as stable as Hyperledger Besu's, which has a pre-defined closing block time.

The experimental results provide valuable insights into the performance of the evaluated blockchain platforms. The advantage of using the PoA consensus protocol over PoW is noteworthy, especially regarding the stability and consistency of results. While Hyperledger Besu and Hyperledger Fabric demonstrate a more predictable and constant behavior, Ethereum exhibits greater variability, suggesting potential scalability challenges. Additionally, the results indicate that PoA tends to offer faster response times compared to PoW, highlighting its potential for applications requiring near real-time responses. In the case of Hyperledger Fabric, even when using the default consensus mechanism, an implementation of Raft, the results exceed those of Hyperledger Besu and Ethereum. As demonstrated in Fig. 4(b), for real-world scenarios where predictability and stability are essential, Hyperledger Fabric has a lesser



(a) TPS for the execution of access control function in smart contract.

(b) TPS for the execution of logging function in smart contract.

(c) Gas accumulation ratio per block relative to the number of transactions in a block.

Fig. 3 Performance of access control and logging policy smart contracts. (**a**) For the access control function, the Hyperledger Besu platform exhibited performance, on average, 100 times higher than Ethereum. (**b**) For the logging function, Hyperledger Besu also shows significant improvement over Ethereum. On average, Hyperledger Fabric overcomes Hyperledger Besu and Ethereum in both functions. (**c**) Hyperledger Besu also demonstrates lower computational cost per block for logging operations compared to Ethereum

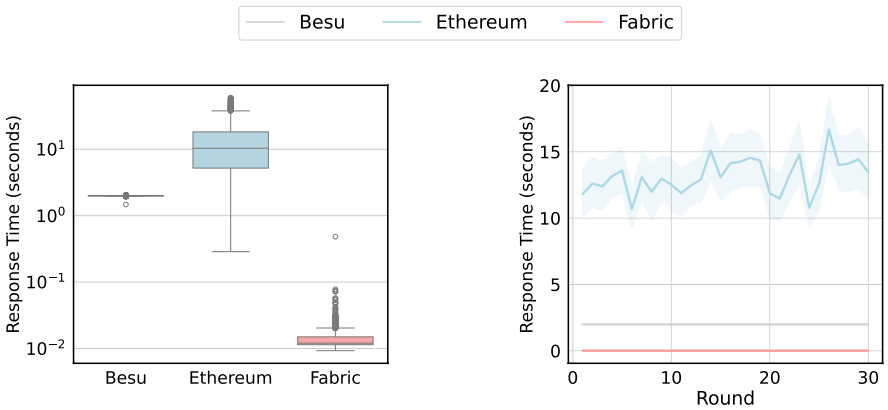


Fig. 4 Performance in resource request response time

(a) Response Time (RT), in seconds, required to request a resource on Besu, Ethereum and Fabric.

(b) Response Time (RT) in seconds per execution round.

impact on response time, which can be crucial for critical applications.

Finally, it is worth highlighting that Hyperledger Fabric outperforms Hyperledger Besu and Ethereum in terms of transactions per second and response time, thanks to its permissioned architecture. This design enables the use of lightweight and efficient consensus protocols, such as a version of Raft that leverages trusted network participants for improvements. Also, Fabric's "execute-order-validate" transaction model enables parallel execution, thereby enhancing scalability. In contrast, Ethereum's sequential "order-execute" model can create performance bottlenecks.

Additionally, Fabric's modular architecture supports private channels and does not rely on a native cryptocurrency, which reduces overhead and speeds up transaction finality. These design choices make Fabric significantly more efficient in controlled environments. In summary, while Ethereum and Besu are tailored for open and decentralized networks, which come with inherent performance trade-offs, Fabric prioritizes performance, control, and privacy, making it particularly well suited for enterprise applications. These assessments provide a solid foundation for understanding the performance of different blockchain platforms and guide future decisions in the evolution and implementation of blockchain-based access control systems.

6 Limitations

The SmartMed system currently faces five main technical constraints concerning identity management, data sovereignty, policy deployment, security evaluation and and real-World systems integration.

1. **Identity Management**: Access revocation and attribute updates primarily rely on external identity managers, as Keycloak, for instance, only consumes data from federated identity providers. Direct user attribute management within the SmartMed system presents a significant challenge, largely due to the granularity limitations inherent in existing identity provider models. Furthermore, it is crucial to highlight that access revocation can occur in two primary ways: first, by updating the policy smart contract to include a new rule that withdraws profile access–a partial solution that involves only system managers and bypasses user participation. The second option involves updating user attributes, which subsequently affects policy evaluation. While this latter approach allows for user involvement in the revocation process, this ideal scenario is not currently implemented in SmartMed.
2. **Data Sovereignty**: Currently, the SmartMed system faces challenges in ensuring full user data sovereignty, as users lack direct control over their attributes and how their data is managed post-access. This limitation inherently affects privacy protection regarding assets and user data. To address this, and consequently enhance the system's privacy protection concerning assets and user data, future work on the SmartMed system will involve integrating with a Decentralized Identity (DID) platform built on the Hyperledger Fabric blockchain. This enhancement will resolve the constraint of users lacking direct control over their attributes and will enable more robust access revocation mechanisms through the implementation of Self-Sovereign Identity (SSI) within SmartMed.
3. **Policy Deployment**: The current process for deploying smart contracts occurs through the native interfaces of the blockchain platform, demanding a solid understanding of the platform's architecture and its specific programming language. This inherent complexity poses a significant challenge to the agile development, rigorous

testing, and efficient deployment of new policies, particularly in a dynamic environment. In future work, SmartMed aims to incorporate a dedicated interface for policy deployment, thereby significantly improving the system's capability to update its access control policies more efficiently.

4. **Security Evaluation**: The current version of SmartMed does not include a security evaluation or a systematic analysis of access control enforcement behavior. While the architecture is designed to support tamper-resistance and immutable logging via blockchain, aspects such as resistance to attack vectors, enforcement correctness, and cryptographic robustness were not experimentally verified. These aspects will be addressed in future work, particularly in the context of integrating decentralized identity mechanisms and formal policy verification tools.
5. **Real-World Systems Integration**: Although SmartMed has been implemented as a minimum viable product and supports containerized deployment via Docker and Kubernetes, this work does not report on real-world integration with existing healthcare systems. Important practical concerns such as legacy system compatibility, staff training, and policy harmonization across institutions have not been addressed. Future work should include pilot deployments in real hospital environments to validate usability, compliance, and integration overhead under realistic operational constraints.

7 Conclusion

The paper investigated the potential of blockchain and distributed ledger technologies to manage access to medical data, provide a reliable platform for storing logs, and establish self-sovereign identity in the field of Digital Health. To this end, the paper extended the SmartMed system and developed a prototype of an access control system integrated with the Keycloak authenticator. Analysis of the prototype revealed that blockchain, especially supported by the Hyperledger Fabric distributed ledger platform, offers security, immutability, audibility, and privacy of health data at a computationally viable cost for its application. Future work aims to integrate Self-Sovereign Identities into SmartMed, enabling users to manage their attributes effectively. Furthermore, SmartMed plans to enhance its scalability, enabling health system managers to deploy and administer policies through an integration interface.

Author Contributions Conceptualization, D.M.F.M., D.S.V.M. and M.T.O.; methodology, D.M.F.M. and D.S.V.M.; validation, D.M.F.M., D.S.V.M. and N.R.O.; investigation, D.M.F.M. and D.S.V.M.; resources, D.M.F.M. and D.S.V.M.; writing—original draft preparation, A.C.R.M. and N.R.O.; writing—review and editing, D.M.F.M., D.S.V.M., N.R.O., A.C.R.M., R.V., Y.R.S., G.N.N.B., L. H. A. R. and M.T.O.; visualization, N.R.O.; supervision, R.V., D.M.F.M. and D.S.V.M.; project administration,D.M.F.M. and D.S.V.M.; funding acquisition, D.M.F.M. and D.S.V.M. All authors have read and agreed to the published version of the manuscript.

Funding This work was supported by CNPq, FAPERJ, RNP, CAPES, and the Municipality of Niterói/FEC/UFF (Edital PDPA 2020) and INCT ICoNIoT (CNPq and CAPES).

Data Availibility Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Competing Interests The authors declare no competing interests.

Consent to Participate Not applicable.

Consent for Publication Not applicable.

Ethics Approval Not applicable.

References

1. Popa, M., Stoklossa, S.M., Mazumdar, S.: Chaindiscipline - towards a blockchain-iot-based self-sovereign identity management framework. IEEE Trans. Serv. Comput. **16**(5), 3238–3251 (2023). https://doi.org/10.1109/TSC.2023.3279871
2. Sahi, N., Liang, A., Van Devanter, W., Oikonomou, K., Zhang, P.: Self-sovereign identity in semi-permissioned blockchain networks leveraging ethereum and hyperledger fabric. In: 2023 IEEE International Conference on Digital Health (ICDH), pp. 315–321 (2023). https://doi.org/10.1109/ICDH60066.2023.00053
3. Spanakis, E.G., Politis, I., Markakis, E., Papatsaroucha, D., Grammatopoulos, A.V., Bolgouras, V., Angelogianni, A., Xenakis, C., Sakkalis, V.: Towards building a self-sovereign identity framework for healthcare. In: 2023 45th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC), pp. 1–4 (2023). https://doi.org/10.1109/EMBC40787.2023.10340626
4. Oliveira, N.R., Santos, Y.d.R., Barbosa, G.N.N., Reis, L.H.A., Mendes, A.C.R., Oliveira, M.T., Medeiros, D.S.V., Mattos, D.M.F.: Distributed data security in digital health: Self-sovereign identity, access control, and blockchain-based log records. In: 2024 6th International Conference on Blockchain Computing and Applications (BCCA), pp. 558–565 (2024). https://doi.org/10.1109/BCCA62388.2024.10844453
5. Albeyatt, A.: Medicalchain white paper 2.1. Technical report, MedChain White Paper 2.1 (September 2018). https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf
6. Anderson, J.: Securing, standardizing, and simplifying electronic health record audit logs through permissioned blockchain technology. UNTHRR (2018)
7. Zhang, P., White, J., Schmidt, D.C., Lenz, G., Rosenbloom, S.T.: FHIRChain: applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotechnol. J. **16**, 267–278 (2018)
8. Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B.: Ancile: Privacy-preserving framework for access control and

interoperability of electronic health records using blockchain technology. Sustainable Cities and Society **39**, 283–297 (2018)
9. Shah, S.M., Khan, R.A.: Secondary use of electronic health record: Opportunities and challenges. IEEE Access **8**, 136947–136965 (2020). https://doi.org/10.1109/ACCESS.2020.3011099
10. De Oliveira, M.T., Reis, M.T., Amorim, L.H., Verginadis, Y., Mattos, D.M.F., Olabarriaga, S.D.: SmartAccess: Attribute-based access control system for medical records based on smart contracts. IEEE Access **10**, 117836–117854 (2022). https://doi.org/10.1109/ACCESS.2022.3217201
11. Telenti, A., Jiang, X.: Treating medical data as a durable asset. Nat. Genet. **52**(10), 1005–1010 (2020)
12. Xu, S., Ning, J., Li, Y., Zhang, Y., Xu, G., Huang, X., Deng, R.H.: A secure emr sharing system with tamper resistance and expressive access control. IEEE Trans. Dependable Secure Comput. **20**(1), 53–67 (2023). https://doi.org/10.1109/TDSC.2021.3126532
13. Sookhak, M., Jabbarpour, M.R., Safa, N.S., Yu, F.R.: Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. J. Netw. Comput. Appl. **178**, 102950 (2021). https://doi.org/10.1016/j.jnca.2020.102950
14. de Oliveira, M.T., Verginadis, Y., Reis, L.H.A., Psarra, E., Patiniotakis, I., Olabarriaga, S.D.: AC-ABAC: Attribute-based access control for electronic medical records during acute care. Expert Syst. Appl. **213**, 119271 (2023). https://doi.org/10.1016/j.eswa.2022.119271
15. Galdi, C., Soltani, R., Nguyen, U.T., An, A.: A survey of self-sovereign identity ecosystem. Security and Communication Networks **2021**, 8873429 (2021). https://doi.org/10.1155/2021/8873429
16. Siqueira, A., Da Conceição, A.F., Rocha, V.: Performance evaluation of self-sovereign identity use cases. In: 2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), pp. 135–144 (2023). https://doi.org/10.1109/DAPPS57946.2023.00026
17. Shuaib, M., Alam, S., Alam, M.S., Nasir, M.S.: Self-sovereign identity for healthcare using blockchain. Materials Today: Proceedings **81**, 203–207 (2023)
18. Oliveira, N. R. d., Santos, Y. d. R. d., Mendes, A. C. R., Barbosa, G. N. N., Oliveira, M. T. d., Valle, R., Medeiros, D. S. V., Mattos, D. M. F.: Storage standards and solutions data storage sharing and structuring in digital health A brazilian case study. Information **15**(1), 20 (2024). https://doi.org/10.3390/info15010020
19. Mattos, D.M.F., Carrara, G.R., Albuquerque, C., Mossé, D.: Exploring overlay topology cost-termination tradeoff in blockchain vicinity-based consensus. IEEE Trans. Netw. Serv. Manage. **20**(2), 1733–1744 (2023)
20. Carrara, G.R., Burle, L.M., Medeiros, D.S.V., Albuquerque, C.V.N., Mattos, D.M.F.: Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking. Ann. Telecommun. **75**(3), 163–174 (2020)
21. Mattos, D.M.F., Medeiros, D.S.V.D., Passos, D., Fernandes, N.C., Muchaluat-Saade, D.C., Moraes, I.M., Albuquerque, C.V.D.: Blockchain for smart grid security: Applications, trends, and challenges. Int. J. Intell. Syst. Technol. Appl. **20**(4), 296–309 (2021)
22. Sutradhar, S., Karforma, S., Bose, R., Roy, S., Djebali, S., Bhattacharyya, D.: Enhancing identity and access management using hyperledger fabric and oauth 2.0: A block-chain-based approach for security and scalability for healthcare industry. Internet of Things and Cyber-Physical Systems **4**, 49–67 (2024)
23. Melo, C., Gonçalves, G., Silva, F.A., Soares, A.: A comprehensive hyperledger fabric performance evaluation based on resources capacity planning. Cluster Computing **27**(9), 12395–12410 (2024)
24. Vijayakumar, P., Rajkumar, S., Sivaraman, A., Jayarekha, P., Chandra sekaran, S.: Drug traceability and health monitoring system with hyperledger fabric. In: International Conference on Blockchain and Trustworthy Systems, pp. 169–183 (2024). Springer
25. Yang, G., Lee, K., Lee, K., Yoo, Y., Lee, H., Yoo, C.: Resource analysis of blockchain consensus algorithms in hyperledger fabric. IEEE Access **10**, 74902–74920 (2022)
26. Rebello, G.A.F., Camilo, G.F., Souza, L.A.C., Potop-Butucaru, M., Amorim, M.D., Campista, M.E.M., Costa, L.H.M.K.: A survey on blockchain scalability: From hardware to layer-two protocols. IEEE Communications Surveys & Tutorials (2024). https://doi.org/10.1109/COMST.2024.3376252
27. Agrawal, D., Minocha, S., Namasudra, S., Gandomi, A.H.: A robust drug recall supply chain management system using hyperledger blockchain ecosystem. Comput. Biol. Med. **140**, 105100 (2022)
28. Yin, J., Xiao, Y., Feng, J., Yang, M., Pei, Q., Yi, X.: Didtrust: Privacy-preserving trust management for decentralized identity. IEEE Transactions on Dependable and Secure Computing (2024). https://doi.org/10.1109/TDSC.2024.3524760
29. Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., Conti, M.: A survey on decentralized identifiers and verifiable credentials. IEEE Communications Surveys & Tutorials (2025). https://doi.org/10.1109/COMST.2025.3543197
30. Hao, J., Gao, J., Xiang, P., Zhang, J., Chen, Z., Hu, H., Chen, Z.: Tdid: Transparent and efficient decentralized identity management with blockchain. In: 2023 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 1752–1759 (2023). https://doi.org/10.1109/SMC53992.2023.10394499
31. Xie, T., Gai, K., Yu, J., Zhu, L., Xiao, B.: SLVC-DIDA: Signature-less Verifiable Credential-based Issuer-hiding and Multi-party Authentication for Decentralized Identity (2025). arXiv:2501.11052
32. Javed, I.T., Alharbi, F., Bellaj, B., Margaria, T., Crespi, N., Qureshi, K.N.: Health-id: A blockchain-based decentralized identity management for remote healthcare. Healthcare (2021). https://doi.org/10.3390/healthcare9060712
33. Rafid, F.A., Benissan, E., Murr, L., Ermakov, I., Oikonomou, K., Zhang, P.: A decentralized identity system for accelerating medical communications within rare disease communities. In: 2022 IEEE International Conference on Blockchain, Smart Healthcare and Emerging Technologies (SmartBlock4Health), pp. 1–8 (2022). https://doi.org/10.1109/SmartBlock4Health56071.2022.10034646
34. Alnour, A.M., Kim, K.H.: Decentralized identifiers (dids)-based authentication scheme for smart health care system. In: 2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 433–438 (2022). https://doi.org/10.1109/ICUFN55119.2022.9829562

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.