Exploration of Digital Health Technologies
Open Exploration

Open Access Systematic Review

Do you need a blockchain in healthcare data sharing? A tertiary review

Kun Li[1*], Ashish Rajendra Sai[2], Visara Urovi[1]

[1]Institute of Data Science, Maastricht University, 6229 EN Maastricht, The Netherlands
[2]Department of Advanced Computing Sciences, Maastricht University, 6229 EN Maastricht, The Netherlands

***Correspondence:** Kun Li, Institute of Data Science, Maastricht University, Paul-Henri Spaaklaan 1, 6229 EN Maastricht, The Netherlands. k.li@maastrichtuniversity.nl
Academic Editor: Carl Asche, University of Utah Health, USA
Received: February 10, 2024 **Accepted:** April 25, 2024 **Published:** June 14, 2024

Cite this article: Li K, Sai AR, Urovi V. Do you need a blockchain in healthcare data sharing? A tertiary review. Explor Digit Health Technol. 2024;2:101–23. https://doi.org/10.37349/edht.2024.00014

Abstract

Background: This study addresses the complexities of utilizing blockchain technology in healthcare, aiming to provide a decision-making tool for healthcare professionals and policymakers evaluating blockchain's suitability for healthcare data sharing applications.

Methods: A tertiary review was conducted on existing systematic literature reviews concerning blockchain in the healthcare domain. Reviews that focused on data sharing were selected, and common key factors assessing blockchain's suitability in healthcare were extracted.

Results: Our review synthesized findings from 27 systematic literature reviews, which led to the development of a refined decision-making flowchart. This tool outlines criteria such as scalability, integrity/immutability, interoperability, transparency, patient involvement, cost, and public verifiability, essential for assessing the suitability of blockchain in healthcare data sharing. This flowchart was validated through multiple case studies from various healthcare domains, testing its utility in real-world scenarios.

Discussion: Blockchain technology could significantly benefit healthcare data sharing, provided its application is carefully evaluated against tailored criteria for healthcare needs. The decision-making flowchart developed from this review offers a systematic approach to assist stakeholders in navigating the complexities of implementing blockchain technology in healthcare settings.

Keywords

Blockchain, healthcare data sharing, decision-making, systematic literature review

Introduction

Blockchain technology has received considerable attention as a potentially transformative innovation through cryptocurrency [1]. However, skepticism has grown regarding its practical, real-world applications, particularly beyond cryptocurrencies and associated use cases [2]. In healthcare, specifically, the promises of blockchain technology may not have materialized yet despite academic surveys highlighting its potential for enhancing data sharing, security, and decentralization of patient information [3].

One primary concern is the lack of real-world applications, as noted in the literature [4]. This lack of practical examples hinders the ability of healthcare professionals to fully understand and evaluate the applicability of blockchain technology in the healthcare domain. Additionally, the implementation of blockchain technology is often characterized by inherent complexity [5]. A case in point is the concept of decentralization within the blockchain, which lacks standardized definitions and a clear understanding [6]. The absence of comprehensive guidelines and frameworks exacerbates these issues, leaving healthcare professionals and policymakers uncertain regarding the suitability and potential trade-offs of adopting blockchain technology [5]. Addressing these gaps is crucial for informed decision-making and effective integration of blockchain.

Existing research articles, such as [3, 7], exploring blockchain in a healthcare context, present potential use cases and discuss areas where blockchain could be advantageous. However, these articles often need a more transparent framework for decisively determining the appropriateness of blockchain technology for a given healthcare issue. The absence of a systematic decision-making process may be a challenge faced by healthcare professionals and policymakers in establishing the relevance of blockchain in the healthcare domain. In this study, we aim to answer the following question:

- Which decision-making criteria are important in assessing the suitability of blockchain technology for sharing healthcare data?

To answer this question, we developed a novel conceptual framework and decision-making flowchart that assists healthcare stakeholders in understanding the usefulness of blockchain technology in healthcare settings. Building upon the work of Wüst and Gervais [8], we conducted a tertiary review of 27 systematic literature reviews (SLRs) focusing on blockchain in healthcare data sharing. This review analyzes existing literature, identifying critical criteria for assessing the suitability of blockchain solutions in healthcare data sharing.

By extracting insights from prior research, we devise a comprehensive decision-making framework to assist the understanding of the trade-offs associated with using blockchain in a healthcare context. The developed framework considers the following essential factors:

- The necessity of data sharing.
- Trusted third-party replacement.
- Data integrity and immutability.
- Transparency in information processing.
- Relevant actors.
- Patient involvement.
- Cost.
- Public verifiability.

This study provides three critical contributions to the understanding and application of blockchain technology in healthcare data sharing: First, it offers insights into the criteria that can influence the use of blockchain in a healthcare context; second, it translates these criteria into apparent, relevant factors for the healthcare sector; lastly, it introduces a flowchart that guides healthcare stakeholders in systematically evaluating the adoption of blockchain technology. By following the flowchart and responding to a series of questions, stakeholders can navigate the decision-making process more structured and better understand blockchain's applicability to their specific use case.

Blockchain technology is a decentralized digital ledger that records transactions across multiple computer nodes in such a way that the verified transactions cannot be altered. Transactions can be seen as the exchange of valuable information between two actors (from a sender to a receiver).

While conceptually rooted in its application in cryptocurrencies [9], blockchain technology exhibits various characteristics that make it a versatile and potential solution for various applications across domains [10, 11]. These characteristics define its operational mechanics and contribute to its growing popularity and adoption in fields like healthcare, finance, and supply chain management [10]. The following are the key characteristics that underscore the potential and versatility of blockchain technology:

- Decentralization. Blockchain operates on a decentralized network architecture, which reduces the dependency on central authorities, enhancing system resilience and integrity [12].
- Immutability. Once data is recorded in a blockchain, it is difficult to alter. This immutability ensures the integrity of the transaction ledger, making blockchain a robust platform for secure transactions [13].
- Transparency and Anonymity. While transactions are transparent and traceable in the blockchain network, the participants' identities are protected through complex cryptographic techniques, which balances transparency and anonymity [14].
- Enforceable agreements. In blockchain technology, transactions are checked for validity via Smart contracts. Smart contracts are self-executing contracts with terms of agreements directly written into code. They run on the blockchain, allowing transactions to be executed automatically when certain conditions are met without intermediaries. This feature facilitates trustless agreements, reduces the potential for disputes, and enhances the efficiency of transactions [15].

The key characteristics of blockchain technology lay the foundation for its diverse applications. However, implementing these characteristics can vary significantly depending on different use cases' specific requirements and constraints. This variability has led to several types of blockchain networks, each tailored to meet unique access, control, speed, and privacy needs. The types of blockchain networks can be categorized into public permissionless, public permissioned, and private blockchains:

- Public permissionless blockchains: Public permissionless blockchains, or public blockchains, are fully decentralized, with no single entity owning the network. They are open to anyone joining and participating in the core activities of the blockchain network, such as validating and recording transactions. Well-known examples include Bitcoin and Ethereum. These networks are characterized by their high transparency and security but often face challenges in terms of scalability and throughput [16].
- Private blockchains: Private blockchains are permissioned networks with access restricted to specific members. Due to their greater control over participants' activities, organizations often use them for internal purposes. This type of blockchain is suited for scenarios requiring privacy and faster transaction speeds but lacks extensive decentralization [17].
- Public permissioned blockchains: A public permissioned blockchain, or consortium blockchain, is a semi-decentralized type where organizations govern the network. This model combines elements of both private and public blockchains. It is often used in business collaborations where multiple stakeholders require control and shared access. Consortium blockchains are ideal for industries like banking, supply chain, and healthcare, where data privacy and shared governance are essential [18].

Blockchain technology has gained attention in various sectors, including healthcare [19]. The features of blockchain, such as decentralization, transparency, and immutability, present novel solutions to challenges in this domain [3, 20].

The application of blockchain technology in healthcare can be categorized into a comprehensive, multidimensional taxonomy, reflecting the technology's versatility in addressing various sector-specific challenges:

- Healthcare data management: Blockchain technology provides innovative solutions for managing, storing, and sharing healthcare data, including electronic health records (EHRs) and electronic medical records (EMRs) [21, 22]. It distributes data across a network with the decentralization feature, enhancing patient control and privacy. Immutability and transparency ensure that once data is recorded, it cannot be altered, maintaining the integrity of patient information, and facilitating interoperability between healthcare systems [23–26]. For example, by leveraging the immutable and transparent nature of blockchain, Azaria et al. [27] proposed a blockchain-based system designed to revolutionize the management and accessibility of EMRs, ensuring secure, patient-centered management of EMRs with seamless sharing across providers.

- Pharmaceutical supply chain and healthcare logistics: In this domain, blockchain enhances the transparency of drug manufacturing and delivery processes, allowing for real-time tracking and verification of pharmaceutical products, organ transplants, and blood donations [21]. Immutability provides a tamper-proof record of each step in the supply chain, ensuring product authenticity and safety [24, 25]. As an example, Huang et al. [28] introduce Drugledger, a blockchain-based system designed to enhance the traceability and regulation of drugs across the supply chain. The system addresses the limitations of traditional centralized approaches by offering a decentralized solution that ensures data authenticity, resilience, and flexibility.
- Interoperability and consolidated healthcare systems: Blockchain technology promotes decentralization to remove intermediaries in data exchange, creating a unified view of patient data across healthcare providers [21]. Transparency ensures this data is accessible and consistent across platforms, improving care coordination and outcomes. For example, Yue et al. [29] propose a novel architecture, Healthcare Data Gateway (HDG), that leverages blockchain technology to empower patients to own, control, and share their healthcare data without compromising privacy. By leveraging a unified data schema and purpose-centric access control, this architecture facilitates the organization and sharing of healthcare data across different systems and stakeholders.
- Clinical trials and medical research: In clinical trials, immutability safeguards the integrity of data collection, patient recruitment, and results dissemination, preventing unauthorized changes and ensuring reliability [21, 23, 25]. Transparency fosters trust in the research process by making methodologies and findings accessible for verification, which is significant for biomedical research and education. As an example, Zhang et al. [30] present FHIRChain, a blockchain-based architecture tailored for the secure and scalable sharing of clinical data in healthcare. Addressing the "Shared Nationwide Interoperability Roadmap" requirements from the Office of the National Coordinator for Health Information Technology, FHIRChain integrates Health Level Seven International's Fast Healthcare Interoperability Resources (FHIR) standard within a blockchain framework to ensure interoperable, privacy-preserving, and secure data exchange.
- Remote care and Internet of Things (IoT) architectures: By integrating with IoT devices, blockchain enhances security through cryptographic protocols and smart contracts against unauthorized data access [23, 24]. Decentralization enables the efficient aggregation of patient data from multiple sources, placing patients at the center of their care, even in remote settings. For example, Azbeg et al. [31] present a healthcare system, BlockMedCare, designed to address security and privacy challenges in remote patient monitoring. The proposed system integrates IoT with blockchain technology to create a secure, scalable, and efficient system for managing chronic diseases that require continuous monitoring. The system leverages proxy re-encryption and smart contracts for access control. It employs the InterPlanetary File System (IPFS) for off-chain data storage to ensure scalability and reduce the processing time associated with data management.
- Health insurance and claims processing: Blockchain streamlines the claims process with smart contracts that execute automatically upon meeting predefined conditions, reducing opportunities for fraud and improving efficiency [21, 25]. Transparency provides clear, auditable trails of transactions, fostering trust among patients, providers, and insurers. Karmakar et al. [32] introduce a blockchain-based framework, ChainSure, for automating and enhancing the security of health insurance systems. By leveraging smart contracts and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) method, this framework automates the insurance process, minimizes

administrative overhead, and provides a transparent and secure platform for transactions between insurers, healthcare providers, and patients.

- Governance: Across the applications, the immutability and transparency of blockchain ensure a secure, unchangeable record of transactions, supporting compliance and governance through reliable audit trails and access controls [26, 33]. For example, Urovi et al. [34] introduced a blockchain-based platform, License accoUntability and CompliancE (LUCE), to support data sharing for research. Using dynamic consent mechanisms [35], the authors automate the management of consent and purpose of use for health-related datasets. In general, by utilizing smart contracts, LUCE provides a secure and transparent method to monitor and enforce compliance with data sharing agreements, thereby overcoming issues related to trust and legal clarity in data reuse.

The taxonomy of blockchain applications in healthcare data sharing is summed up in Table 1.

Table 1. The taxonomy of blockchain applications in healthcare

Category	Description	Blockchain properties supporting the applications
Healthcare data management	Management, storage, and sharing of electronic health records (EHRs) and electronic medical records (EMRs). Enhancing patient data control and interoperability	Transparency Immutability Decentralization
Pharmaceutical supply chain and healthcare logistics	Ensuring authenticity, traceability, and safety of pharmaceutical products, organ transplants, and blood donations	Transparency Immutability
Interoperability and consolidated healthcare systems	Creating a unified view of patient data across healthcare providers to improve care coordination and outcomes	Transparency Decentralization
Clinical trials and medical research	Securing data collection, patient recruitment, and results sharing for clinical trials. Supporting reliability and verifiability of medical research	Immutability Transparency
Remote care and Internet of Things (IoT) architectures	Real-time patient monitoring, secure data collection, and remote healthcare delivery through integration with IoT devices	Enforceable agreements Decentralization
Health insurance and claims processing	Automating and securing health insurance claims processing via smart contracts. Reducing fraud and streamlining the claims lifecycle	Enforceable agreements Transparency
Governance	Ensuring health data security and privacy across applications through cryptographic methods. Providing audit trails, access control, and data aggregation for governance	Immutability Transparency Enforceable agreements Decentralization

Pilot projects and theoretical models have attempted to use blockchain in healthcare [8], but have faced challenges in scalability, integration with existing systems, and regulatory compliance [36]. These mixed outcomes reflect the early nature of blockchain application in healthcare and illustrate the need for a more nuanced understanding of the practicality of these technologies.

Blockchain technology has emerged as a pivotal innovation in healthcare, offering secure, immutable, transparent, and decentralized solutions for dealing with a wide array of data types [21, 36]:

- Clinical and laboratory data: Blockchain systems provide a platform that supports the sharing of patient data, including clinical data, laboratory results, and medical imaging [36]. By integrating blockchain technology, healthcare providers can ensure the integrity and confidentiality of patient data, facilitating seamless access and interoperability across different healthcare systems [36].
- Medical claims and cost data: The management of insurance claims and associated cost data benefits from blockchain technology [25]. Through smart contracts, blockchain systems can automate the claims processing workflow, reducing fraud, eliminating intermediaries, and ensuring transparency in the billing and payment process [21].

- Patient-generated data: With the increasing use of IoT devices in healthcare [25], blockchain serves as a backbone for securely managing the vast amounts of data generated by these devices, ensuring the integrity and security of data collected from wearable devices, home monitoring systems, and other IoT applications [37]. Additionally, blockchain technology empowers patients by giving them control over their healthcare data, facilitating real-time monitoring and personalized care interventions.
- Pharmaceutical and organ data: Blockchain's application extends to managing pharmaceutical data and organ donation records [21, 33]. It ensures the authenticity of pharmaceutical products, tracks their distribution, and manages organ donor registries and transplant records. By providing a tamper-proof ledger for these sensitive data types, blockchain technology can combat counterfeit drugs and streamline organ donation processes.

Although data security encompasses a range of challenges, blockchain-based applications mainly focus on addressing three areas: ensuring data integrity, managing access control, and preserving privacy [38]:

- Ensuring data integrity: Data integrity is paramount in healthcare to maintain the accuracy and completeness of healthcare data overtime [39]. Blockchain technology enhances data integrity in healthcare by creating a decentralized and tamper-evident record system. Every transaction on the blockchain is timestamped and linked to the previous transaction, forming a chronological chain. This feature makes unauthorized alterations evident and allows for easy verification of data history [40].
- Managing access control: Access control in healthcare is critical for protecting patient privacy and ensuring that sensitive healthcare data is only accessible to authorized individuals [41]. In blockchain-based healthcare applications, users can innovatively manage access control through smart contracts [35]. These are self-executing contracts with the terms of the agreement directly written into code, enforcing who can access what data under which circumstances automatically.
- Preserving privacy: Privacy preservation is essential in healthcare due to the sensitive nature of the data involved [42]. The transparency of blockchain introduces complexities in ensuring privacy; however, cryptographic techniques such as zero-knowledge proofs enable the verification of data without exposing the underlying details [43]. Integrating blockchain with advanced cryptographic technologies like proxy re-encryption further enhances privacy [44, 45]. This technique allows encrypted data to be re-encrypted for a new recipient without decrypting it first. Additionally, decentralized privacy-preserving identity mechanisms can be employed to protect individual identities [46]. These mechanisms operate through blockchain, ensuring that while data remains traceable, the identities behind the data are safeguarded without central authority oversight, providing a robust framework for privacy.

Managing healthcare data is a complex process with various application domains, data types, and security objectives [7]. Issues like data breaches, unauthorized access, and the inefficiency of traditional centralized systems highlight the vulnerability of current healthcare data management practices [5]. The sensitive nature of health data requires a system that ensures privacy and security while maintaining accessibility and accuracy [7].

Despite the growing body of literature on blockchain in healthcare, there remains a disconnect between theoretical research and real-world application [8]. This gap is partly from the early nature of blockchain technology and the complexity of healthcare systems. Current research often focuses on potential use cases without adequately addressing the practical challenges of implementing blockchain solutions in diverse healthcare environments [47].

Given the complexities and the early stage of blockchain research and applications in healthcare, there is a critical need for a structured decision-making framework [48]. Such a framework would assist healthcare stakeholders in evaluating the feasibility and appropriateness of blockchain technology in specific healthcare contexts [49].

Materials and methods

This section outlines the materials and methods employed to develop and validate the decision-making framework. We conducted a tertiary review [50] of SLRs that focus on blockchain and healthcare data sharing. Following this review, we perform data extraction and analysis to refine the flowchart initially proposed by Wüst and Gervais [8]. Our primary goal is to analyze and synthesize the findings of multiple SLRs to establish a comprehensive understanding of the current state of knowledge in this field. Through this tertiary review, we aim to identify key themes and challenges present in the existing literature concerning the application of blockchain in healthcare data sharing. Figure 1 shows the overall methodology steps used for selecting papers and extracting data.

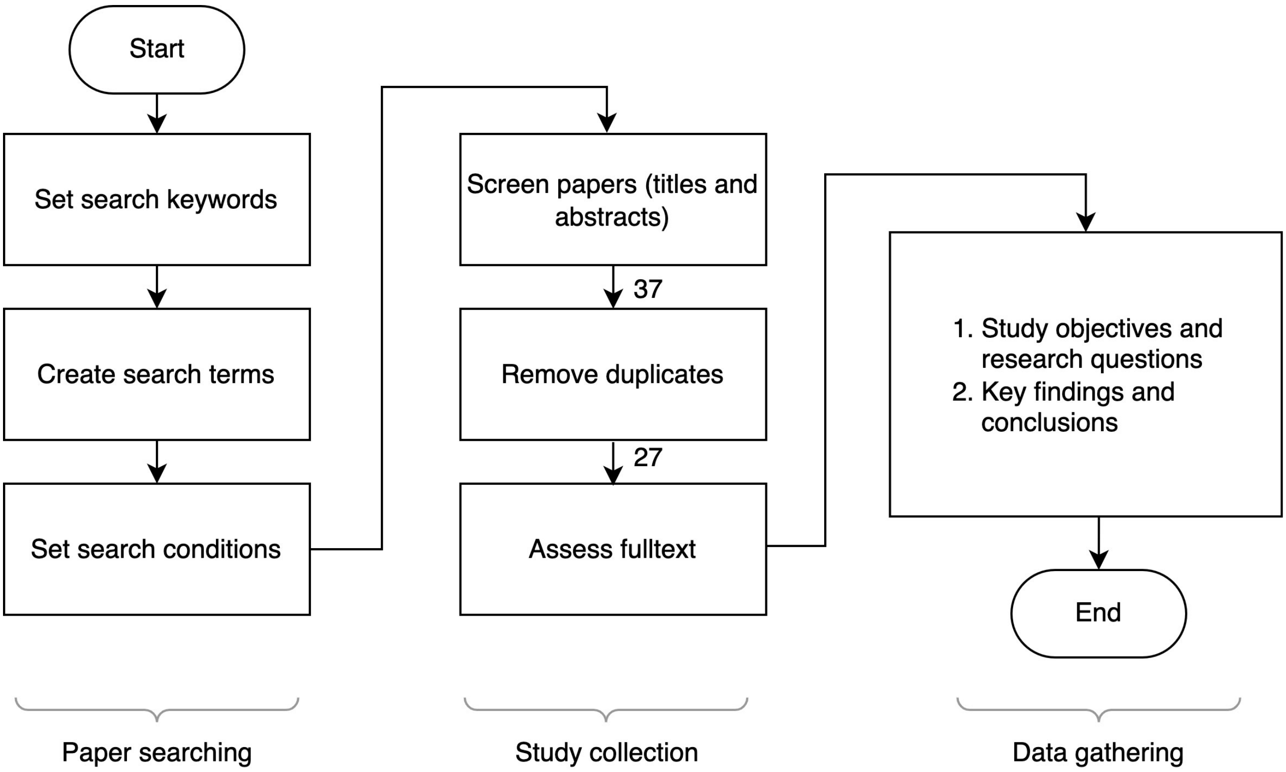

Figure 1. Overview of the methodology

Search strategy

To identify relevant SLRs focusing on the application of blockchain technology in healthcare, we developed a comprehensive search strategy, which involved a systematic and structured search across various databases and sources to ensure a thorough coverage of the topic.

Data sources

We conducted searches in several electronic databases recognized for their comprehensive coverage of literature in the fields of technology and healthcare. These included:

- PubMed
- IEEE Xplore
- ACM Digital Library
- Science Direct
- Springer Link

Additionally, to ensure exhaustive coverage and capture literature that might not be indexed in the aforementioned databases, we conducted supplementary searches in:

- Google Scholar

Search terms and strategy

The development of the search strategy involved an integration of specific keywords and Boolean logic. The core search terms employed were "blockchain", "healthcare", and "systematic literature review". These terms were interconnected using Boolean operators. For instance, the search query "blockchain" AND "healthcare" AND "systematic literature review" was utilized. To ensure compatibility with the unique indexing systems and search functionalities of each database, the search queries were customized accordingly. The temporal scope of the search was confined to the period from 2008, marking the publication of Bitcoin's white paper, to December 2023, the knowledge cutoff date of this study. The retrieved articles were then listed according to their relevance to the search purposes.

Study selection

As shown in Table 2, the initial results were screened based on titles and abstracts to identify studies that potentially met our inclusion criteria. The inclusion criteria were:

- Articles focusing on the application of blockchain in healthcare.
- Studies that were SLRs.
- Publications in English.

Table 2. The results were screened by titles and abstracts

Data sources	Search results
PubMed	10
IEEE Xplore	6
ACM Digital Library	1
Science Direct	3
SpringerLink	2
Google Scholar	15
Total	37

Exclusion criteria included:

- Non-peer-reviewed articles.
- Articles not relevant to the core focus of blockchain in healthcare.
- Studies lacking a systematic approach in methodology.

Then, the duplicates were removed using digital object identifiers (DOIs).

Data extraction and management

To answer the research question proposed, selected articles underwent a full-text review for detailed analysis. Relevant information was extracted and compiled into a predefined data extraction template, which included:

- Study objectives and research questions.
- Key findings and conclusions.

Results

In this section, we present the results of our tertiary review, outlining the specific criteria used to assess the suitability of blockchain technology for sharing healthcare data. Building upon the flowchart by Wüst and Gervais [8], we have developed a refined version that enhances precision, focus, and comprehensibility, specifically tailored for healthcare practitioners.

Criteria for blockchain application in healthcare data sharing

In examining the applicability of blockchain technology for healthcare data sharing, our analysis identified eight critical criteria: scalability, privacy, integrity/immutability, interoperability/accessibility, transparency, patient involvement, legal compliance, and cost/incentive, as shown in Table 3. These criteria, combined with the flowchart by Wüst and Gervais [8], collectively form a comprehensive framework, guiding the evaluation of blockchain's application in healthcare data sharing.

Table 3. Criteria and decision points for blockchain application in healthcare data sharing

Criteria	Decision point	Reference
Scalability	Can you share via trusted third parties?	[21, 25, 51–55]
Privacy	Are all actors trusted?	[21, 25, 26, 51, 54, 56, 57]
Integrity/immutability	Is data integrity and immutability crucial?	[21, 22, 38, 39, 54, 56–65]
Interoperability/accessibility	Are the identities of actors known?	[21, 25, 51, 52, 54, 55, 58, 61, 66, 67]
Transparency	Is transparency towards actors important?	[57, 61–65]
Patient involvement	Do you need to involve patients?	[25, 58]
Legal compliance	Is public verifiability required?	[21, 54, 67]
Cost/incentive	Is cost a limiting factor?	[21, 26, 55, 67]

Do you need a blockchain in healthcare data sharing? A flowchart

Determining the suitability of blockchain technology for healthcare applications requires a systematic evaluation of various factors. To address this, we have developed a comprehensive decision-making flowchart, as shown in Figure 2.

The flowchart serves as a valuable tool for healthcare practitioners, facilitating informed decision-making regarding the implementation of blockchain solutions. It encompasses factors such as the requirements of data sharing, data integrity, and immutability, the identity verification and trustworthiness of healthcare actors, patient involvement, and public verifiability. Each step of the flowchart is accompanied by three elements, a rationale, term definitions, and a decision pathway. The rationale explicates the purpose of each step, ensuring that stakeholders understand the importance of the considerations involved. Term definitions are provided to clarify technical and healthcare-specific terminology, catering, especially to practitioners less familiar with blockchain technology. Finally, the decision pathway guides users to subsequent steps based on their specific circumstances and requirements.

Step 1: Do you need to share data?

1. Rationale
   This initial question focuses on the necessity of data sharing. It serves as the primary filter for assessing the applicability of blockchain in the health domain.
2. Term definition
   "Data" refers to information that is relevant to the health domain, often related to the physical, mental, and social well-being of individuals or populations. This encompasses a wide range of data types including, but not limited to, medical histories, diagnostic results, treatment information, and lifestyle specifics [21].
3. Decision pathway
   If a healthcare organization does not have a requirement to share data, the integration of blockchain may not offer substantial benefits. Thus, this question lays the foundation for the subsequent inquiries and decision-making processes.

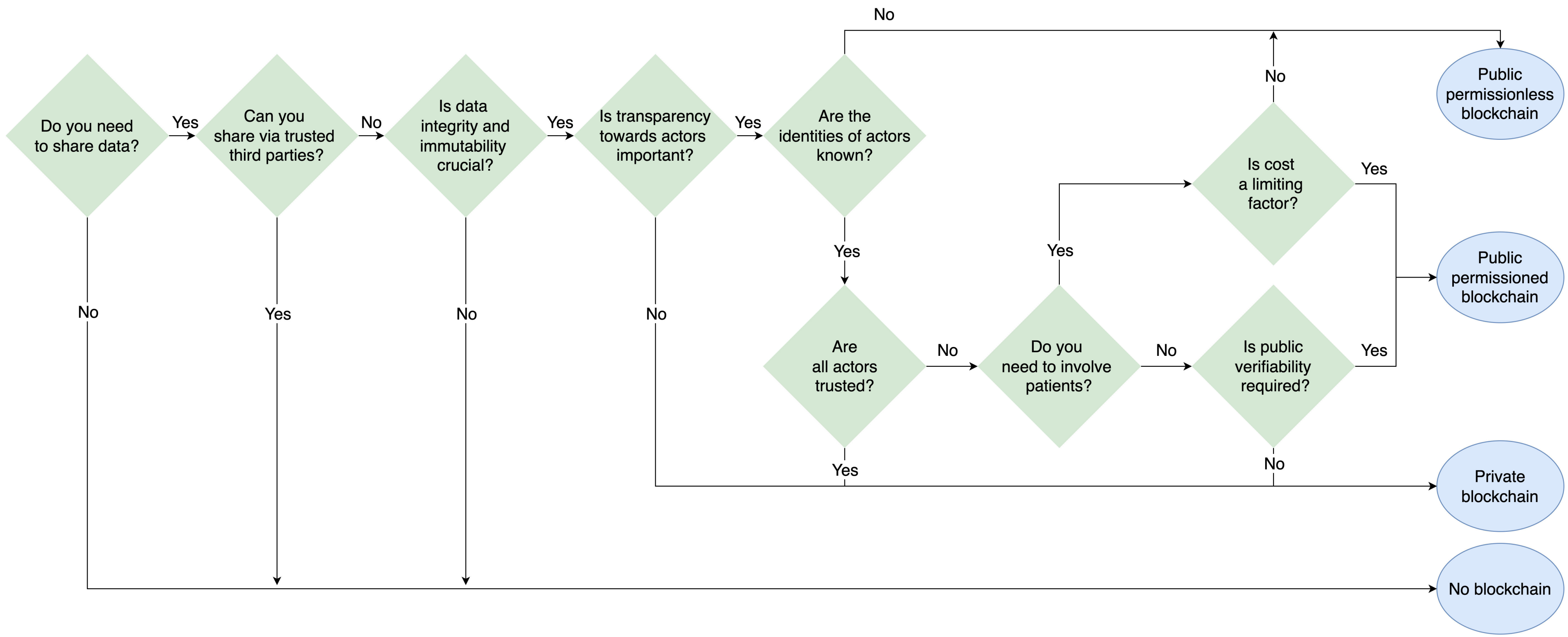

Figure 2. The decision-making flowchart

Step 2: Can you share via trusted third parties?

1. Rationale

   This step examines the necessity of trusted third parties in traditional and centralized healthcare data sharing systems [68], such as hospitals, insurance companies, and government agencies. It directly confronts the scalability challenge of transitioning traditional, centralized healthcare data sharing to a decentralized blockchain approach [21, 51, 52]. This step also prompts an evaluation of whether the existing infrastructure, predominantly based on trusted third parties, meets the demands of healthcare data sharing. It invites stakeholders to assess the scalability challenge of current blockchain technology. The decision to integrate blockchain in healthcare should consider scale and balance the benefits of decentralization against the established trust in centralized systems.

2. Term definition
   "Trusted third party" refers to centralized entities responsible for storing, processing, and sharing health information [25].
3. Decision pathway
   In the healthcare sector, trusted third parties offer established systems for data sharing, yet this comes with potential drawbacks, including increased vulnerability to data breaches, alongside a shift in control and trust towards these entities. On the other hand, blockchain technology provides a decentralized framework, ensuring data owners maintain ownership over their data, dictating access and sharing terms. This approach may mitigate trust and data security concerns; however, as a novel technology, it is challenged by efficiency and difficulties in integrating with existing healthcare systems. Therefore, if sharing via trusted third parties is possible, sharing with the support of blockchain technology may be unnecessary. This is particularly true if high transaction speed is required. However, if there is a need to scale data sharing to multiple actors and a trusted third-party model is not possible or not available, then a blockchain model could contribute.

Step 3: Is data integrity and immutability crucial?

1. Rationale
   In this step, data integrity and immutability ascend to paramount importance [57, 63, 65]. This step prompts stakeholders to consider whether the existing data sharing mechanisms afford sufficient control over the data's integrity once it is out of their direct custody. It challenges them to evaluate if traditional systems offer adequate safeguards against unauthorized alterations, deletions, or breaches.
2. Term definitions
   "Data integrity" entails the accuracy and consistency of data over its lifecycle [38]. "Data Immutability", on the other hand, refers to the data's unchangeability once recorded, preventing unauthorized alterations that could compromise its reliability [62].
3. Decision pathway
   - If data integrity and immutability are not deemed crucial for a specific healthcare data sharing scenario, the necessity for employing blockchain technology is reduced. In these cases, the complexities and costs associated with implementing a blockchain solution may not be justified because the data in question does not significantly impact patient care outcomes, regulatory compliance, or where traditional database systems provide sufficient security and audit capabilities.
   - When data integrity and immutability are crucial in this context, blockchain technology emerges as a pivotal solution. Blockchain's inherent features, such as decentralized storage, cryptographic hashing, and consensus algorithms, provide a potential solution when maintaining control over data integrity and immutability is a primary concern in data sharing scenarios.

Step 4: Is transparency towards actors important?

1. Rationale
   Transparency is not just a preference but a necessity in modern healthcare data management [69, 70]. It fosters trust among stakeholders [63] and aids in compliance with regulatory standards [48]. Given the sensitive nature of healthcare data, stakeholders must be assured that the data is handled appropriately and that activities are traceable and accountable [55].
2. Term definition
   "Actors" refers to all individuals and entities interacting with the shared data, including patients, healthcare providers, insurance companies, administrators, and possibly others like researchers or pharmaceutical companies [55, 59].

"Transparency" within a healthcare system refers to the extent of access and visibility offered to various stakeholders. Generally, it includes a transparent and auditable record of one or many of the following: data access, processing, and sharing. In the context of blockchain-based systems, the level of transparency varies depending on the type of blockchain [63]. This transparency ensures that all actions are conducted with integrity and align with established protocols and regulations [55].

3. Decision pathway
   When evaluating blockchain integration for healthcare data sharing, it is essential to assess the necessity of transparency across all healthcare actors, thereby guiding the selection of the blockchain type.

   - For environments where transparency needs are balanced with privacy concerns, a private permissioned blockchain could be more appropriate. Such a blockchain allows for selective visibility of transactions, ensuring only authorized parties can access specific data. It supports regulatory compliance and protects sensitive information while offering transparency to those granted access.
   - Conversely, in a scenario where transparency is required to build trust and ensure accountability among all actors, exploring a public permissioned or permissionless blockchain might be advisable. It provides an open environment where data transactions are visible to anyone, enhancing transparency but requiring careful consideration of privacy and data sensitivity.

Step 5: Are the identities of actors known?

1. Rationale
   In healthcare scenarios where the identities of the actors are known, the data sharing is typically limited to a few organizations identifying a solution to share information. In other health scenarios, the identities of the actors are not well known due to a need for information sharing across multiple organizations. In this later case, the information is generated or collected in different technical systems thereby, interoperability becomes an important concept linked to this question. Therefore, identifying actors within a data-sharing network aligns with ensuring interoperability, which is significant in healthcare [71, 72]. Interoperability, in this context, refers to the ability of different entities to communicate, exchange data, and use the information that has been exchanged efficiently and effectively based on the identification of healthcare actors [73]. This step underscores the importance of interoperable systems in ensuring that the identities of all participants in the healthcare data sharing process are accurately known and verifiable. The level of identity disclosure directly impacts the appropriate blockchain type [74].
2. Term definition
   "Known identities" implies that the real-world identities of these actors are verified and authenticated within the system [74].
3. Decision pathway
   Identifying all participants is crucial for determining the type of blockchain when integrating it into healthcare data sharing.

   - If the identities of all actors do not need to be publicly known or verified, a public permissionless blockchain may be considered. It allows for anonymous or pseudonymous participation, facilitating a broader engagement. However, interoperability may be challenging where identity verification is necessary.
   - On the other hand, if verifying the identities of all healthcare actors is essential, a public permissioned blockchain would be more suitable. This approach supports interoperability by enabling secure, authenticated interactions across different actors. It also ensures that each

actor's identity is known and verified, enhancing trust and compliance with healthcare regulations.

Step 6: Are all actors trusted?

1. Rationale
Trust among actors in a healthcare data-sharing context is important to ensure that the data is not misused and that all parties adhere to the agreed-upon protocols and ethical standards. In a blockchain network, trust can be related to confidence in the actors' behavior and the security of the transactions [24, 75]. The level of trust among the actors will influence the governance model and the degree of decentralization appropriate for the blockchain system [6, 76].
2. Term definitions
"Trusted actors" refers to entities and individuals that have established a record of reliability and ethical handling of healthcare data. Trust can be derived from historical interactions, reputation, or regulatory compliance [71]. In blockchain terms, this might translate into the need for less stringent consensus mechanisms or the ability to operate with a higher degree of autonomy within the network [55, 59].
3. Decision pathway
    - If all actors are trusted, a private blockchain might be sufficient. It could be suitable for a group of healthcare providers or between trusted entities with existing relationships. It leverages the inherent trust to ensure data security and compliance while benefiting from advantages like immutability and transparency. It is sufficient for controlled, secure data exchange, where wide-scale decentralization is less critical, allowing for efficient and streamlined operations within the trusted network.
    - If there is a mix of trusted and untrusted actors, or if trust needs to be established through system architecture, a public permissioned blockchain may be necessary with further consideration. It allows for a more controlled environment than a public permissionless blockchain, which balances between openness and the need for specific restrictions. It requires actors to have permission to join, which can help main security and trustworthiness while still leveraging the benefits of blockchain technology to ensure data integrity.
    - In cases where no actor is fully trusted, a public permissionless blockchain might be employed, combining further filtering factors. Here, trust is not placed on any single actor but on the blockchain protocol and the distributed network of participants to maintain integrity. This approach ensures transparency and accountability, making it suitable for scenarios requiring high levels of trust and security without centralized control.

Step 7: Do you need to involve patients?

1. Rationale
In healthcare, patient-centric care models are increasingly important, and involving patients in their data management is a key aspect of this [77]. Patient involvement can empower individuals to take control of their health information, allowing them to grant or revoke access to their data [78, 79]. Blockchain can offer a platform where patients can actively engage with their data securely and transparently [80].
2. Term definition
"Patient involvement" refers to the participation of patients in managing and controlling access to their healthcare data. It includes viewing their medical records, sharing them with healthcare providers, and possibly contributing data from wearables or other personal health devices [78, 81]. Patient involvement could be direct or indirect. Direct patient involvement refers to sharing

information directly, empowering patients to manage and control access to their healthcare data actively. Indirect patient involvement refers to the data sharing being pseudonymous or anonymous, where direct identifiers are removed from healthcare data to protect patient privacy, and data owners retain a mapping between the identities of patients and their de-identified records.

3. Decision pathway
   - If patient involvement is required, a public permissionless or permissioned blockchain could be suitable, combined with further discussion. Such blockchains facilitate patient interaction with their healthcare data and allow patients to claim ownership of their healthcare data, placing them at the center of healthcare data sharing.
   - If patient involvement is not required, a private blockchain or a public permissioned blockchain may be adequate, where healthcare providers or administrators hold control over data access and management, facilitating efficient data sharing and management within the healthcare sector. It focuses on operational efficiency and compliance with regulatory standards without requiring direct patient involvement in the data sharing process.

Step 8: Is cost a limiting factor?

1. Rationale
   Cost is a significant consideration for healthcare organizations when integrating blockchain technology, which can vary widely depending on the network type and the implementation scale [4]. The decision balances the financial resources available with the benefits a blockchain solution could provide.
2. Term definition
   "Cost" in the context of integrating blockchain technology in healthcare data sharing encompasses the financial expenditure required for the system's initiation and maintenance, including upfront investment needed for hardware, software, and expert labor and the recurrent costs like energy consumption, system upgrades, and security measures. In the context of blockchain, transaction fees should also be considered. These are necessary considerations in deciding the type and scale of blockchain implementations suitable for healthcare organizations [3].
3. Decision pathway
   - If cost is a limiting factor, a public permissioned blockchain might be more appropriate, leading to lower operational and infrastructure expenses due to restricted access and optimized network requirements.
   - In cases where the budget allows for a more robust and decentralized solution, and the benefits of such a solution outweigh the costs, a public permissionless blockchain could be considered. Public permissionless blockchains stand out for their open and decentralized nature, leading to higher operational costs due to the extensive computational power needed to validate transactions and maintain the network.

Step 9: Is public verifiability required?

1. Rationale
   Public verifiability is an important factor in the choice of blockchain architecture, especially in the healthcare sector, where the integrity of data and the accountability of actors are subject to scrutiny by external parties [54, 67]. In such scenarios, the blockchain's inherent audibility feature becomes invaluable, as it provides a tamper-proof ledger where all transactions are recorded in a manner that is secure and accessible for verification purposes. The decision here will largely depend on the nature of the data being shared and the broader objectives of the healthcare organization regarding public trust and accountability [8].

2. Term definition
   "Public verifiability" means the capability of any external party, without necessarily being part of the blockchain network, to validate the data and transactions on the blockchain [8]. This feature is critical in ensuring transparency and integrity of data, where the public or independent entities can audit and confirm the legitimacy of the information stored on the blockchain [8].
3. Decision pathway
   - If public verifiability is a requirement, indicating that the recorded data is of public interest and not sensitive, a public permissioned blockchain is likely an appropriate choice. It allows for public verification while controlling access and maintaining some level of privacy and security, fostering transparency and trust, particularly in public health data or research findings.
   - In cases where public verifiability is not essential, or data sensitivity necessitates more restricted access, a private blockchain might be more suitable. This blockchain limits verifiability to specific, authorized parties, offering a controlled environment while maintaining security and privacy.

Evaluating the suitability of blockchain in healthcare: case studies

To evaluate the utility of our decision-making flowchart in guiding blockchain implementation decisions within the healthcare sector, we analyze MedRec [27], Drugledger [28], iWellChain [82], DACIL [83], REALM [84], ChainSure [32], and LUCE [85], as shown in Table 4. In this table, the category column classifies each project into functional areas. The case description provides brief summaries of each project's objectives. Assumptions detail the underlying premises for each project's evaluation, focusing on aspects like data privacy and cost distribution. The decision path outlines the step-by-step choices made based on the decision-making flowchart, indicating decisions with 'Yes' or 'No'. Finally, the final outcome column shows the type of blockchain technology adopted by each project. Detailed analysis can be found in Supplementary material.

To have a more comparative understanding of our decision-making framework, we integrate the case studies into the original flowchart, as shown in Figure 3. The color-coded paths indicate different routes that can be taken depending on the answers to the yes/no questions at each decision point. These paths represent distinct case studies, each with unique considerations and endpoints.

Discussion

Implications of the results for healthcare professionals and policymakers

The findings of this review, resulting in a decision-making flowchart for determining the suitability of blockchain in healthcare applications, have significant implications for healthcare professionals and policymakers.

For healthcare professionals, the flowchart serves as a valuable tool for assessing the potential benefits and challenges of integrating blockchain into their practice. It guides them in considering factors such as the necessity of data sharing, trusted third parties, date immutability and integrity, participant knowledge, patient involvement, and public verifiability. By leveraging blockchain technology in appropriate scenarios, healthcare professionals can enhance data security and privacy, improve interoperability, and enhance patient care coordination [3]. Understanding the conditions under which blockchain is most likely to yield positive outcomes is essential for effective utilization by healthcare professionals.

Policymakers can also benefit from the insights provided by this study to develop appropriate regulations and guidelines regarding the implementation of blockchain in healthcare. The flowchart offers policymakers a comprehensive understanding of the factors to consider when assessing the feasibility associated with adopting blockchain technology. Policymakers can utilize this information to shape policies that support innovation while ensuring privacy, security, and ethical use of blockchain in healthcare. Additionally, they can address legal and regulatory challenges that may arise, promoting responsible and effective integration of blockchain in the healthcare ecosystem [86].

Table 4. Case studies of evaluating the suitability of blockchain applications in healthcare

Category	Case description	Assumptions	Decision path	Final outcome
Healthcare data management	MedRec—enables patients a comprehensive, immutable log and convenient access to their medical information across providers and treatment sites	No	1-Yes, 2-No, 3-Yes, 4-Yes, 5-Yes, 6-No, 7-Yes, 8-Yes	Public permissioned blockchain
Pharmaceutical supply chain and healthcare logistics	Drugledger is designed to enhance traceability and regulation throughout the drug supply chain	Prioritize operational efficiency and long-term sustainability over initial cost	1-Yes, 2-No, 3-Yes, 4-Yes, 5-Yes, 6-No, 7-Yes, 8-Yes	Public permissioned blockchain
Interoperability and consolidated healthcare systems	iWellChain—is designed to improve data sharing among healthcare providers and patients, ensuring data interoperability and security	Transaction costs are paid by the users initiating transactions, allowing them to operate without incurring the full burden of the network costs, and distributing it among users	1-Yes, 2-No, 3-Yes, 4-Yes, 5-Yes, 6-No, 7-Yes, 8-No	Public permissionless blockchain
Clinical trials and medical research	DACIL—to define decision support and a digital companion to aid patients (and their caregivers) during lung attacks. The project requires trials to collect user data and to have them interact with the platform	Phase 1: User's data and some previously collected cohorts will be stored on a trusted platform. Few data analysts will have access to the data Phase 2: The investigators would like to find a way to share data later with the broader research community	Phase 1: 1-Yes, 2-Yes Phase 2: 1-Yes, 2-No, 3-Yes, 4-Yes, 5-No	Initially, blockchain is not needed. When sharing broadly, a public permissionless blockchain would help to better control the data
Remote care and Internet of Things (IoT) architectures	REALM—aims to define a monitoring platform in support of the health Artificial Intelligence (AI) software certification process	In order to test health AI software, special data needs to be used. Health data is not shared but the outcomes of the tests on the AI models should be seen and trusted by all the members of the REALM network. No trusted third party can be used	1-Yes, 2-No, 3-Yes, 4-Yes, 5-Yes, 6-No, 7-No, 9-Yes	REALM requires a public permissioned blockchain for public verifiability
Health insurance and claims processing	ChainSure—aims to create a decentralized, tamper-proof system for health insurance management. It automates policy selection, claims processing, and data sharing, thereby reducing administrative overhead and enhancing data integrity	Transaction costs are paid by the users initiating transactions, allowing them to operate without incurring the full burden of the network costs, and distributing it among users	1-Yes, 2-No, 3-Yes, 4-Yes, 5-Yes, 6-No, 7-Yes, 8-No	Public permissionless blockchain
Governance	License accoUntability and CompliancE (LUCE)—is designed to facilitate compliance with data licensing terms and General Data Protection Regulation (GDPR) requirements through a blockchain solution	Transaction costs are paid by the users initiating transactions, allowing them to operate without incurring the full burden of the network costs, and distributing it among users	1-Yes, 2-No, 3-Yes, 4-Yes, 5-Yes, 6-No, 7-Yes, 8-No	Public permissionless blockchain

Identification of gaps in the current literature and areas for future research

This review has also identified gaps and areas for future research in the healthcare blockchain field. While the literature on this topic has expanded, certain aspects require further investigation.

Firstly, more empirical studies are needed to evaluate blockchain solutions' actual implementation and impact in real-world healthcare settings. While existing literature provides theoretical insights and frameworks, empirical evidence of blockchain applications' effectiveness, efficiency, and user experiences in healthcare is limited. Future research should focus on conducting expert interviews, stakeholder surveys, and pilot projects to assess the practical implications, challenges, and benefits of implementing blockchain technology across various healthcare domains and organizational contexts.

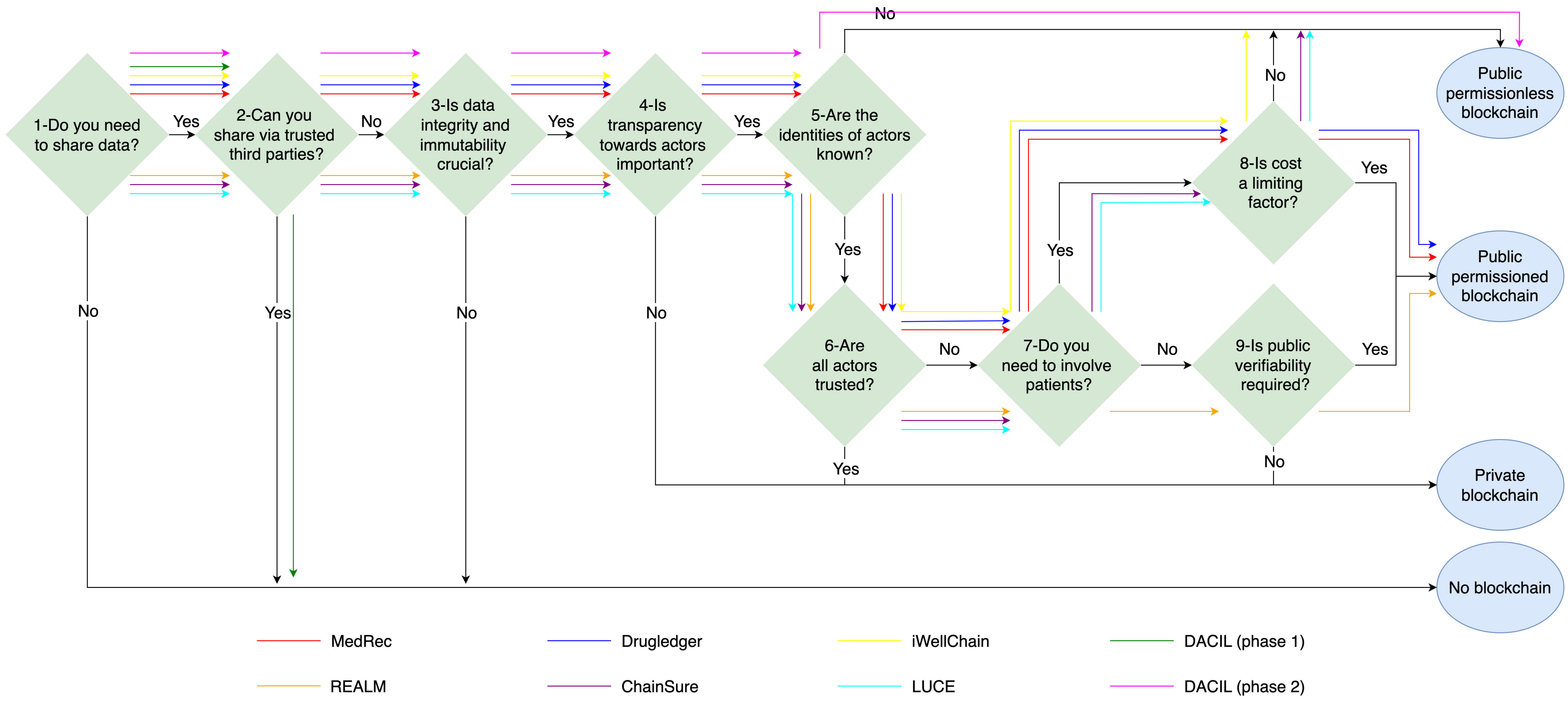

Figure 3. Case studies of the decision-making flowchart

Secondly, blockchain's ethical, legal, and social implications in healthcare require further exploration. As blockchain technology becomes more prevalent in healthcare, examining ethical considerations related to patient privacy, data ownership, consent management, and data governance is crucial. Additionally, legal and regulatory frameworks should be developed to address unique challenges posed by blockchain, such as jurisdictional issues, liability, and dispute resolution. Future research should provide comprehensive guidance on the ethical and legal aspects of blockchain implementation, facilitating responsible and transparent use of the technology in healthcare.

Furthermore, as the volume and complexity of healthcare data continue to rise, the scalability of blockchain solutions becomes a critical concern. Scalability in this context refers to the ability of blockchain networks to handle increasing amounts of data without compromising on speed or efficiency. Efficient data processing is crucial in healthcare, where real-time data availability can significantly impact patient care and outcomes. Future research needs to focus on enhancing the scalability of these networks through innovative approaches such as sharding, which divides the network into smaller, more manageable segments, or through layer two solutions that process transactions off the main blockchain to decrease load and increase speed. This will ensure that as healthcare data grows, blockchain networks remain efficient and responsive to the needs of the industry.

Lastly, interoperability between blockchain platforms and existing healthcare systems is critical for successfully adopting and implementing blockchain technology in healthcare. This interoperability involves the seamless integration and exchange of data across different blockchain platforms, blockchain networks, and legacy healthcare systems. The challenge lies in creating a standardized framework for secure, reliable, and efficient data exchange. Future studies should explore the development of technical solutions and standards that facilitate this integration. Adopting common standards can significantly enhance the potential for blockchain to support diverse healthcare applications, from patient records management to supply chain transparency, thereby improving healthcare delivery.

Limitations of the review and suggestions for improving future studies

Despite employing a rigorous methodology, this review has some limitations. Firstly, it relies on existing SLRs as the primary source of information, which may vary in quality and coverage. To address this, future studies could consider incorporating primary research studies to complement findings from SLRs.

Secondly, the validation of the decision-making flowchart is currently conducted using case studies, primarily due to constraints in time and resources. To enhance the validity of the flowchart in future iterations, future studies should incorporate a broader range of methods, such as expert interviews, stakeholder surveys, and pilot projects. These additional methods will gather diverse perspectives and more comprehensive feedback, contributing significantly to developing a more robust and reliable decision-making tool.

Lastly, the decision-making flowchart presented in this study is based on synthesizing existing literature. It may not capture all possible factors or considerations relevant to specific healthcare contexts. Therefore, healthcare professionals and policymakers should contextualize the flowchart within their unique organizational settings and critically reflect before making decisions about adopting blockchain technology.

In conclusion, this tertiary review underscores the potential benefits and complexities of integrating blockchain technology in healthcare. The study developed and validated a decision-making flowchart to assist healthcare professionals and policymakers in making informed decisions about blockchain applications in healthcare. The flowchart, tested through various case studies, offers a structured approach to evaluating the viability and implications of blockchain technology. Our findings stress the necessity of assessing key factors such as scalability, privacy, interoperability, and legal compliance to harness blockchain's benefits effectively. The inclusion of practical case studies confirms the applicability of the decision-making tool across various healthcare domains, promoting a responsible and informed approach to adopting blockchain technology in the healthcare sector.

Abbreviations

EMRs: electronic medical records

IoT: Internet of Things

LUCE: License accoUntability and CompliancE

SLRs: systematic literature reviews

Supplementary materials

The supplementary material for this article is available at: https://www.explorationpub.com/uploads/Article/file/101114_sup_1.pdf.

Declarations

Author contributions

KL: Conceptualization, Investigation, Writing—original draft, Writing—review & editing. ARS: Conceptualization, Writing—original draft, Writing—review & editing. VU: Conceptualization, Writing—review & editing, Supervision. All authors read and approved the submitted version.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Ethical approval

Not applicable.

Consent to participate

Not applicable.

Consent to publication

Not applicable.

Availability of data and materials

The datasets that support the findings of this study are available from the corresponding author upon reasonable request.

Funding

This work was partially funded by the following grants: the China Scholarship Council [202109650003]. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Copyright

References

1. Cong LW, He Z. Blockchain Disruption and Smart Contracts. Rev Financ Stud. 2019;32:1754–97.
2. Zīle K, Strazdiņa R. Blockchain Use Cases and Their Feasibility. Appl Comput Syst. 2018;23:12–20.
3. Attaran M. Blockchain technology in healthcare: Challenges and opportunities. Int J Healthc Manag. 2022;15:70–83.
4. AbuHalimeh A, Ali O. Comprehensive review for healthcare data quality challenges in blockchain technology. Front Big Data. 2023;6:1173620.
5. O'Donoghue O, Vazirani AA, Brindley D, Meinert E. Design Choices and Trade-Offs in Health Care Blockchain Implementations: Systematic Review. J Med Internet Res. 2019;21:e12426.
6. Hoffman MR, Ibáñez L-D, Simperl E. Toward a Formal Scholarly Understanding of Blockchain-Mediated Decentralization: A Systematic Review and a Framework. Front Blockchain. 2020;3:35.
7. Yaqoob I, Salah K, Jayaraman R, Al-Hammadi Y. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput Applic. 2022;34:11475–90.
8. Wüst K, Gervais A. Do you Need a Blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). Crypto Valley Conference on Blockchain Technology (CVCBT); 2018 Jun 20-22; Zug, Switzerland. IEEE; 2018. pp. 45–54.
9. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Internet]. [cited 2023 Nov 1]. Available from: https://assets.pubpub.org/d8wct41f/31611263538139.pdf

10. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telemat Inform. 2019;36:55–81.
11. Levis D, Fontana F, Ughetto E. A look into the future of blockchain technology. Plos One. 2021;16: e0258995.
12. Yaga D, Mell P, Roby N, Scarfone K. Blockchain Technology Overview. arXiv: 1906.11078v1 [Preprint]. 2019 [cited 2023 Nov 1]: [68 p.]. Available from: https://arxiv.org/pdf/1906.11078
13. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Gener Comput Syst. 2018;82:395–411.
14. Fernández-Caramés TM, Fraga-Lamas P. A Review on the Use of Blockchain for the Internet of Things. IEEE Access. 2018;6:32979–3001.
15. Taherdoost H. Smart Contracts in Blockchain Technology: A Critical Review. Information. 2023;14: 117.
16. Naaz R, Saxena AK, Shah PK. Blockchain technology's overview: Consensus, architecture and future trends. AIP Conf Proc. 2023;2427:020018.
17. Hawlitschek F, Notheisen B, Teubner T. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electron Commer Res Appl. 2018;29:50–63.
18. Belchior R, Vasconcelos A, Guerreiro S, Correia M. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. ACM Comput Surv. 2021;54:1–41.
19. Mackey TK, Kuo TT, Gummadi B, Clauson KA, Church G, Grishin D, et al. 'Fit-for-purpose?' – challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Med. 2019;17:68.
20. Haleem A, Javaid M, Singh RP, Suman R, Rab S. Blockchain technology applications in healthcare: An overview. Int J Intell Networks. 2021;2:130–9.
21. Soltanisehat L, Alizadeh R, Hao H, Choo K-KR. Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review. IEEE Trans Eng Manage. 2020;70:353–68.
22. Elangovan D, Long CS, Bakrin FS, Tan CS, Goh KW, Yeoh SF, et al. The Use of Blockchain Technology in the Health Care Sector: Systematic Review. JMIR Med Inf. 2022;10:e17278.
23. Merlo V, Pio G, Giusto F, Bilancia M. On the exploitation of the blockchain technology in the healthcare sector: A systematic review. Expert Syst Appl. 2023;213:118897.
24. Saeed H, Malik H, Bashir U, Ahmad A, Riaz S, Ilyas M, et al. Blockchain technology in healthcare: A systematic review. Plos One. 2022;17:e0266462.
25. Agbo CC, Mahmoud QH, Eklund JM. Blockchain Technology in Healthcare: A Systematic Review. Healthcare. 2019;7:56.
26. Chukwu E, Garg L. A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. IEEE Access. 2020;8:21196–214.
27. Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In: 2016 2nd International Conference on Open and Big Data (OBD). International Conference on Open and Big Data (OBD); 2016 Aug 22-24; Vienna, Austria. IEEE; 2016. pp. 25–30.
28. Huang Y, Wu J, Long C. Drugledger: A Practical Blockchain System for Drug Traceability and Regulation. In: 2018 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData). IEEE/ACM Int'l Conference on & Int'l Conference on Cyber, Physical and Social Computing (CPSCom) Green Computing and Communications (GreenCom); 2018 Aug 03-2018 Jul 30; Halifax, NS, Canada. IEEE; 2018. pp. 1137–44.
29. Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J Med Syst. 2016;40:218.

30. Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Comput Struct Biotechnol J. 2018;16:267–78.
31. Azbeg K, Ouchetto O, Andaloussi SJ. BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. Egypt Inf J. 2022;23:329–43.
32. Karmakar A, Ghosh P, Banerjee PS, De D. ChainSure: Agent free insurance system using blockchain for healthcare 4.0. Intell Syst Appl. 2023;17:200177.
33. Hölbl M, Kompara M, Kamišalić A, Nemec Zlatolas L. A Systematic Review of the Use of Blockchain in Healthcare. Symmetry. 2018;10:470.
34. Urovi V, Jaiman V, Angerer A, Dumontier M. LUCE: A blockchain-based data sharing platform for monitoring data License accoUntability and CompliancE. Blockchain Res Appl. 2022;3:100102.
35. Jaiman V, Urovi V. A Consent Model for Blockchain-Based Health Data Sharing Platforms. IEEE Access. 2020;8:143734–45.
36. Khezr S, Moniruzzaman M, Yassine A, Benlamri R. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. Appl Sci. 2019;9:1736.
37. Peng Z, Xu C, Wang H, Huang J, Xu J, Chu X. P^2B-Trace: Privacy-Preserving Blockchain-based Contact Tracing to Combat Pandemics. In: 2021 International Conference on Management of Data. International Conference on Management of Data; 2021 Jun 20-25; China. MOD; 2021. pp. 2389–93.
38. Adere EM. Blockchain in healthcare and IoT: A systematic literature review. Array. 2022;14:100139.
39. Pandey AK, Khan AI, Abushark YB, Alam MM, Agrawal A, Kumar R, et al. Key Issues in Healthcare Data Integrity: Analysis and Recommendations. IEEE Access. 2020;8:40612–28.
40. Chandol MK, Kameswara Rao M. Blockchain-based cryptographic approach for privacy enabled data integrity model for IoT healthcare. J Exp Theor Artif Intell. 2023:1–22.
41. Jiang R, Chen X, Yu Y, Zhang Y, Ding W. Risk and UCON-based access control model for healthcare big data. J Big Data. 2023;10:104.
42. Ali A, Al-Rimy BAS, Alsubaei FS, Almazroi AA, Almazroi AA. HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. Sensors (Basel). 2023;23:6762.
43. Moosa H, Ali M, Alaswad H, Elmedany W, Balakrishna C. A combined Blockchain and zero-knowledge model for healthcare B2B and B2C data sharing. Arab J Basic Appl Sci. 2023;30:179–96.
44. Mittal S, Ghosh M. A three-phase framework for secure storage and sharing of healthcare data based on blockchain, IPFS, proxy re-encryption and group communication. J Supercomput. 2024;80:7955–92.
45. Liu G, Xie H, Wang W, Huang H. A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption. J Cloud Comput. 2024;13:44.
46. Zhou L, Diro A, Saini A, Kaisar S, Hiep PC. Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. J Inf Secur Appl. 2024;80:103678.
47. Ramzan S, Aqdus A, Ravi V, Koundal D, Amin R, Al Ghamdi MA. Healthcare Applications Using Blockchain Technology: Motivations and Challenges. In: IEEE Transactions on Engineering Management. IEEE Transactions on Engineering Management; 2022 Jul 25; 2022. pp. 2874–90.
48. Minssen T, Rajam N, Bogers M. Clinical trial data transparency and GDPR compliance: Implications for data sharing and open innovation. Sci Public Policy. 2020;47:616–26.
49. Ritz D, Althauser C, Wilson K. Connecting Health Information Systems for Better Health: Leveraging interoperability standards to link patient, provider, payor, and policymaker data [Internet]. PATH; 2014 [cited 2023 Nov 1]. Available from: https://www.r4d.org/wp-content/uploads/Connecting-Health-Information-Systems-for-Better-Health.pdf

50. Keele S. Guidelines for performing Systematic Literature Reviews in Software Engineering [Internet]. Kitchenham; 2007 [cited 2023 Nov 1]. Available from: https://www.researchgate.net/profile/Barbara-Kitchenham/publication/302924724_Guidelines_for_performing_Systematic_Literature_Reviews_in_Software_Engineering/links/61712932766c4a211c03a6f7/Guidelines-for-performing-Systematic-Literature-Reviews-in-Software-Engineering.pdf
51. Haddad A, Habaebi MH, Islam MR, Hasbullah NF, Zabidi SA. Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems. IEEE Access. 2022;10:94583–615.
52. Javed W, Aabid F, Danish M, Tahir H, Zainab R. Role of Blockchain Technology in Healthcare: A Systematic Review. In: 2021 International Conference on Innovative Computing (ICIC). International Conference on Innovative Computing (ICIC); 2021 Nov 9-10; Lahore, Pakistan. IEEE; 2021. pp. 1–8.
53. Fang HSA, Tan TH, Tan YFC, Tan CJM. Blockchain Personal Health Records: Systematic Review. J Med Internet Res. 2021;23:e25094.
54. Tandon A, Dhir A, Islam AN, Mäntymäki M. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Comput Ind. 2020;122:103290.
55. Yaqoob S, Khan MM, Talib R, Butt AD, Saleem S, Arif F, et al. Use of Blockchain in Healthcare: A Systematic Literature Review. Int J Adv Comput Sci Appl. 2019;10;644–53.
56. Kiania K, Jameii SM, Rahmani AM. Blockchain-based privacy and security preserving in electronic health: a systematic review. Multimed Tools Appl. 2023:1–27.
57. Kamangar ZU, Memon RA, Murtaza Memon G, Kamangar UA. Integration of Internet of Things and blockchain technology in healthcare domain: A systematic literature review. Int J Commun Syst. 2023; 36:e5582.
58. Hussien HM, Yasin SM, Udzir S, Zaidan AA, Zaidan BB. A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction. J Med Syst. 2019;43:320.
59. Saranya R, Murugan A. A systematic review of enabling blockchain in healthcare system: Analysis, current status, challenges and future direction. Mater Today Proc. 2023;80:3010–5.
60. Alghazwi M, Turkmen F, Van Der Velde J, Karastoyanova D. Blockchain for Genomics: A Systematic Literature Review. Distrib Ledger Technol Res Pract. 2022;1:1–28.
61. Thomson C, Beale R. Is blockchain ready for orthopaedics? A systematic review. J Clin Orthop Trauma. 2021;23:101615.
62. Mayer AH, da Costa CA, Righi RdR. Electronic health records in a Blockchain: A systematic review. Health Informatics J. 2020;26:1273–88.
63. Fatoum H, Hanna S, Halamka JD, Sicker DC, Spangenberg P, Hashmi SK. Blockchain Integration With Digital Technology and the Future of Health Care Ecosystems: Systematic Review. J Med Internet Res. 2021;23:e19846.
64. Lopez-Barreiro J, Alvarez-Sabucedo L, Garcia-Soidan JL, Santos-Gago JM. Use of Blockchain Technology in the Domain of Physical Exercise, Physical Activity, Sport, and Active Ageing: A Systematic Review. Int J Environ Res Public Health. 2022;19:8129.
65. Dubovitskaya A, Novotny P, Xu Z, Wang F. Applications of blockchain technology for data-sharing in oncology: Results from a systematic literature review. Oncology. 2020;98:403–11.
66. Zukaib U, Cui X, Hassan M, Harris S, Hadi HJ, Zheng C. Blockchain and Machine Learning in EHR Security: A Systematic Review. IEEE Access. 2023;11:130230–56.
67. Vazirani AA, O'Donoghue O, Brindley D, Meinert E. Implementing Blockchains for Efficient Health Care: Systematic Review. J Med Internet Res. 2019;21:e12439.
68. Hulsen T. Sharing Is Caring-Data Sharing Initiatives in Healthcare. Int J Environ Res Public Health. 2020;17:3046.

69. Hutchings E, Loomes M, Butow P, Boyle FM. A systematic literature review of health consumer attitudes towards secondary use and sharing of health administrative and clinical trial data: a focus on privacy, trust, and transparency. Syst Rev. 2020;9:235.
70. Boué S, Byrne M, Hayes AW, Hoeng J, Peitsch MC. Embracing Transparency Through Data Sharing. Int J Toxicol. 2018;37:466–71.
71. Kerasidou A, Kerasidou CX. Data-driven research and healthcare: public trust, data governance and the NHS. BMC Med Ethics. 2023;24:51.
72. Kalkman S, Mostert M, Gerlinger C, van Delden JJM, van Thiel GJMW. Responsible data sharing in international health research: a systematic review of principles and norms. BMC Med Ethics. 2019;20:21.
73. Reegu F, Daud SM, Alam S. Interoperability Challenges in Healthcare Blockchain System - A Systematic Review. Ann Rom Soc Cell Biol. 2021:15487–99.
74. Mulaji SS, Roodt SS. The Practicality of Adopting Blockchain-Based Distributed Identity Management in Organisations: A Meta-Synthesis. Secur Commun Networks. 2021;2021:9910078.
75. Zhang R, Xue R, Liu L. Security and Privacy for Healthcare Blockchains. IEEE Trans Serv Comput. 2021;15:3668–86.
76. Schädler L, Lustenberger M, Spychiger F. Analyzing decision-making in blockchain governance. Front Blockchain. 2023;23.
77. Hylock RH, Zeng X. A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study. J Med Internet Res. 2019;21:e13592.
78. de Freitas C, Amorim M, Machado H, Leão Teles E, Baptista MJ, Renedo A, et al. Public and patient involvement in health data governance (DATAGov): protocol of a people-centred, mixed-methods study on data use and sharing for rare diseases care and research. BMJ Open. 2021;11:e044289.
79. Arnstein L, Wadsworth AC, Yamamoto BA, Stephens R, Sehmi K, Jones R, et al. Patient involvement in preparing health research peer-reviewed publications or results summaries: a systematic review and evidence-based recommendations. Res Involv Engagem. 2020;6:34.
80. Westphal E, Seitz H. Digital and Decentralized Management of Patient Data in Healthcare Using Blockchain Implementations. Front Blockchain. 2021;4:732112.
81. McCarron TL, Moffat K, Wilkinson G, Zelinsky S, Boyd JM, White D, et al. Understanding patient engagement in health system decision-making: a co-designed scoping review. Syst Rev. 2019;8:97.
82. Lo YS, Yang CY, Chien HF, Chang SS, Lu CY, Chen RJ. Blockchain-Enabled iWellChain Framework Integration With the National Medical Referral System: Development and Usability Study. J Med Internet Res. 2019;21:e13563.
83. Developing A digital COPD companion for Improving Lifestyle (DACIL) [Internet]. NOW; c2024 [cited 2024 Apr 16]. Available from: https://www.nwo.nl/en/projects/kich1gz0321023
84. Real-world-data enabled assessment for health regulatory decision-making [Internet]. [cited 2024 Apr 16]. Available from: https://realm-ai.eu/
85. Havelange A, Dumontier M, Wouters B, Linde J, Townend D, Riedl A, et al. LUCE: A Blockchain Solution for monitoring data License accoUntability and CompliancE. arXiv:190802287v1. [Preprint]. 2019 [cited 2023 Nov 1]: [14 p.]. Available from: https://arxiv.org/abs/1908.02287
86. Bayle A, Koscina M, Manset D, Perez-Kempner O. When Blockchain Meets the Right to Be Forgotten: Technology versus Law in the Healthcare Industry. In: 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI). IEEE WIC ACM International Conference on Web Intelligence (WI); 2018 Dec 3-6; Santiago, Chile; 2018. pp. 788–92.