# Intelligent Healthcare Data Management using Blockchain: Current Limitation and Future Research Agenda

Alevtina Dubovitskaya[1], Petr Novotny[2], Scott Thiebes[3], Ali Sunyaev[3], Michael Schumacher[4], Zhigang Xu[5], and Fusheng Wang[6]

[1] Lucerne University of Applied Sciences and Arts; Swisscom, Switzerland
[2] IBM T.J. Watson Research Center, USA
[3] Karlsruhe Institute of Technology, Germany
[4] University of Applied Sciences and Arts, Western Switzerland
[5] Stony Brook University Hospital, USA
[6] Stony Brook University, USA

**Abstract.** Healthcare is undergoing a big data revolution, with vast amounts of information supplied from numerous sources, leading to major paradigm shifts including precision medicine and AI driven healthcare among others. Yet, there still exist significant barriers before such approaches could be adopted in practice, including data integration and interoperability, data sharing, security and privacy protection, scalability, policy, and regulations. Blockchain provides a unique opportunity to tackle major challenges in healthcare and biomedical research, such as enabling data sharing and integration for patient-centered care, data provenance allowing verification authenticity of the data, and optimization of some of the healthcare processes among others. Nevertheless, technological constraints of the current blockchain technologies necessitate further research before mass adoption of the blockchain-based healthcare data management is possible. We analyze context-based requirements and capabilities of the available technology and propose a research agenda and new approaches towards achieving intelligent healthcare-data management using blockchain.

**Key words:** Blockchain, Healthcare, Intelligent Data Management

## 1 Introduction

The accelerating digitization of the healthcare sector has led to the creation of large volumes of sensitive data stored online in multiple formats and representations, including electronic health records, medical images, genome sequences, sensor data from monitoring devices, payor records, clinical trials data, and more. Once these data are properly combined, they can be leveraged by data analytics and machine learning techniques to advance the medical, pharmaceutical, sports, and other domains of healthcare-related research and applied medicine. This has inspired the shift of healthcare to precision medicine and AI-driven healthcare.

To combine these data and ensure the input to the intelligent healthcare data-management systems, it is crucial to ensure interoperability between different data sources that often store and process the data in multiple formats. Due to the volumes of the data that are continuously being produced, the difficulty to extract the required information is apparent. The task is further complicated by the intricacies of the highly-regulated and heterogeneous healthcare environment.

Regulations in Europe and the United States, GDPR [1], and HIPAA, [2] advocate patient's privacy: a patient has the right over his/her health information and can set rules and limits on who can access and receive the health information, as well as the right for his/her data erasure. The Office of the National Coordinator for Health Information Technology in the US (ONC) recently announced a proposed rule on interoperability and information blocking, with a strong focus on a patient's ability to access their own electronic health record (EHR) at no cost [3]. Achieving interoperability and privacy simultaneously seem contradictory and hence present a significant challenge. How to guarantee that the data can be easily exchanged and available when required, but in a privacy-preserving way, i.e., that the patient is still able to control who can access his data for which purposes? How can we explicitly prove that the patient has given his consent in an efficient manner?

Ecosystems for health information exchange (HIE) aim to ensure that the data from EHRs are securely, efficiently and accurately shared nationwide. However, HIEs have limited adoption, and there is a lack of standard architecture or protocol to ensure security and enforcement of the access control, specified by patients [4].

The possibility of using emerging blockchain technology for healthcare data management has recently raised major attention in both industry and academia [5, 6, 7, 8]. Blockchain technology can be employed to enable a user with complete control of data and privacy without a central point of control, which will help to accelerate and enhance the privacy-preserving data sharing process. In case of chronic diseases, it is particularly important due to the multiple-medication intake (therefore, drug-to-drug interaction and management of the prescriptions and reimbursements), diagnosis and treatment conducted at multiple hospitals (due to the specialization of centers, required "second opinion", and the mobility of the patients) [5, 9, 10]. Employing blockchain technology can contribute to the optimization of the pharmaceutical supply-chain processes, including clinical trials, and medical research in general [11, 12, 13]. Yet, regardless of ongoing academic research and high interest from the industrial perspective, blockchain-based healthcare data-management systems are not in place yet.

**Contributions:** In this paper, we (i) define domain-specific requirements from the perspective of intelligent healthcare-data management (in Section 2); (ii) introduce blockchain technology and focus on the selection of the *healthcare processes that can benefit from applying blockchain technology*, providing high-level description of the existing approaches, in Section 3. In Section 4, we analyse the limitations of existing works in, often related to the technological restraints

of the blockchain or underlying technologies. Trying to bridge the gap between the domain-specific requirements and technical capabilities, in Section 5, we (iii) propose a *research agenda and new approaches for intelligent healthcare-data management using blockchain*. Section 6 concludes the paper.

## 2 Healthcare requirements and goals

Patient needs to provide his caregiver with the data required for the best treatment outcome. Yet, the patient has a right for privacy. Therefore, the data need to be shared with different entities but following the "privacy-by-design" principle: inline with the patient's will, and not revealing more than required.

The amount of healthcare related data corresponding to a single person frequently grows dramatically. Reliable systems for data storage and management, agnostic to the number of records are required to ensure that a person can maintain a life-long history of his healthcare data.

For the system to comply with the regulations governing personal data (including healthcare data) management in EU or US, each patient needs to provide a consent to share his data for both primary care and research purposes, and has a right for the consent revocation.

Moreover, for primary care, the following security properties are essential: availability of the data, data integrity, and data confidentiality. These properties can be defined as follows:

- *Availability* refers to the ability to use the information or resource when requested. Availability is an important aspect of reliability, as well as of system design [14].
- *Integrity* refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication) [14].
- *Confidentiality* refers to preventing the disclosure of information to unauthorized individuals or systems [15]. Although confidentiality refers to the data, privacy, as defined above, refers to the person and his right to decide to keep his personal data confidential.

*Data anonymization* can be an alternative to consent management when data are shared for research purposes. In practice, in addition to interoperability and compliance with legislation and policies that regulate management of the personal data and, in particular, protected health information, traceability is required.

*Traceability of the data* can be defined as the ability to retain the identities of the origin of the data, the entities who accessed the data, and the operations performed on the data (e.g., updates) [16]. The data traceability will be particularly useful in legal cases, in an audit of care practices, as well as for the patient, in defining and enforcing his access-control policy, in allowing meaningful data aggregation for research purposes, and in enabling reproducibility of research.

Based on the domain specifics and taking into account the sensitive nature of the healthcare data, we can define the following required functionalities of a healthcare data management system:

- Ensure that patients control and can access their information at any time.
- Ensure that the patient must not lose access to his data, or in case it happens, he should be able to recover the access.
- Define mechanism for the healthcare stakeholders, in particular, care providers to access the data in the framework of multiple scenarios: (i) consent is provided by the patient and is easy to verify (for both primary care and research purposes), (ii) emergency situation occurs, and the consent is impossible to obtain, (iii) research is based on only anonymized data (no need for consent), (iv) traceability and audit.

## 3 Applications of blockchain in healthcare

In this section, we first provide a short introduction to the blockchain technology, then, based on the available scientific literature and industry manifesto, we provide a high-level summary of healthcare scenarios and processes, where applying blockchain has been proposed. For each process, we depict the goals and motivations to apply the blockchain technology, mainly focusing on the characteristics and aspects of the current processes that can potentially be improved by employing blockchain: data availability and accessibility, immutability, transparency, security, and privacy, as well as patient involvement in clinical research.

### 3.1 Blockchain overview

Blockchain is a peer-to-peer distributed ledger technology that provides a shared, immutable, and transparent append-only register of all the transactions that happen in the network. It is secured using cryptographic primitives such as hash functions, digital signatures, and encryption algorithms [17]. The data in the form of transactions are digitally signed and broadcasted by the participants, and then grouped into blocks in the chronological order and time-stamped. A hash function is applied to the content of the block and forms a unique block identifier, which is stored in the subsequent block. Due to the properties of the hash function (the result is deterministic and can not be reversed), by hashing the block content again and comparing it with the identifier from the subsequent block, one can easily verify if the content of the block was modified. An ordered sequence of the blocks forms a blockchain ledger.

The blockchain ledger is replicated and maintained by every participant. With this decentralized approach, there is no need for setting up a single trusted centralized entity for managing the registry. The participants can immediately notice a malicious attempt to tamper the information stored in the registry and reject it; hence the immutability of the ledger is guaranteed. The technique of

adding a new block to the existing ledger is defined by the consensus protocol employed in the blockchain technology. Based on how the identity of a participant and its permissions to participate in the consensus are defined within a network, one could distinguish between permissionless and permissioned blockchain systems [18].

Different platforms are employed in the aforementioned approached. A recent review [19] provides an extensive list of studies and ongoing projects that focus using permissionless blockchains in healthcare settings. The authors also discuss potential problems and challenges to be considered when adopting permissionless blockchain technology (e.g., speed and scalability, confidentiality, the threat of a 51% attack, management of the transaction fees and mining). Moreover, the analysis of network traffic can lead to inferring patterns of treatment from frequency analysis of the interactions with the ledger [5].

Membership mechanisms employed in permissioned blockchain platforms allow to control participation in the blockchain network and access to the ledger. While this construction allows to avoid some of the disadvantages of permissionless platforms, permissioned network is more centralized by construction, thus may introduce a threat of single point of failure. Some of the challenges and potential benefits employing permissioned blockchain platforms in healthcare, can be found in Krawiec et al. [20] and in the white paper from IBM [21].

### 3.2 Blockchain healthcare scenarios

Below, we focus on healthcare scenarios where blockchain-based approaches and/or applications have already been proposed. We also reference several notable publications that refer to a more detailed description of the blockchain-based applications within specific clinical data management processes[1].

1. *Connecting healthcare stakeholders and maintaining complete history of patients healthcare data:*
   Blockchain technology can be used to ensure traceability and immutability of the patients healthcare data without putting medical records on the blockchain, but keeping the metadata only, that can also include patient's consent. The voluminous ans sensitive healthcare data can be stored within individual nodes on the network, while their intelligent representations will be stored on-chain [5]. Alternative approach is to use compliant cloud-based service for temporal storage and data exchange (i.e., timeframe defined by the patient) [10]. FHIRchain [9] is a blockchain-based approach for data-sharing that encapsulates HL7 Fast Healthcare Interoperability Resources (FHIR) standard for the clinical data. Efficient on-chain consent management and enforcement of access-control policy expressed by the consent will speed-up and facilitate data sharing for primary care in a privacy-preserving manner.

[1] For a complete overview of the use of blockchain in healthcare, we refer an interested reader to the recent relevant and extensive systematic literature reviews [7, 8]

Better treatment control can be achieved by connecting patients, multiple healthcare providers, health insurer/insurances, and pharmacies and providing them with the specific types of data. One of the barriers for establishing "connected health" is lack of interoperability. Peterson et al. [22] presented a system design based on the permissioned blockchain platform (MultiChain), and discussed how FHIR integration into such system can address the interoperability issue. The proof of interoperability proposed in [22] is based on conformance to the FHIR protocol, which requires verification that the messages sent to the blockchain can get converted to other required formats. Transparent execution of smart-contracts will enable fast, automatized, trustworthy, and bias-free processes reimbursements and claims.
Additionally, it is necessary to ensure compliance with the regulations related to healthcare data management. Magyar in [23] in their theoretical work, based on the principles of the HIPAA regulation, suggests a list of cryptographic tools that can be potentially applied to ensure data privacy and security. Traceability, the authenticity of the data (and sources), and interoperability between data sources will enable a possibility to build and maintain a complete life-long history of healthcare data.

2. *Pharmaceutical supply-chain:* Blockchain-based use cases in supply-chain are emerging, including using traceability and immutability properties of the blockchain to combat counterfeit medicines, securing medical devices, optimizing functionality of healthcare IoT devices, and improving the public health supply chain [24], ensuring control over returned drugs to the pharmaceutical company. In a recent review, Scott et al. demonstrate how blockchain technology can provide functionality that benefits supply chain management in general and traceability of pharmaceuticals in particular [25]. Compliance in pharmaceutical supply-chain, verification of the transportation and storage conditions are of a high importance, e.g., medications can loose their efficiency, if the conditions of storage or transportation are violated. Addressing this issue, Bocek et al. proposed to use smart contracts deployed on the Ethereum blockchain for compliance verification based on the sensor data (i.e., temperature measurements. from a sensor placed in strategical points of the shipment) [13].
3. *Medical research and its reproduceability:* Clinical trials are conducted in order to evaluate new technologies and drugs. Coordination between multiple centers enables to aggregate higher volumes of more heterogeneous data in a shorter period of time, compare to the clinical trials conducted in only one medical institution. Also, involvement of multiple centers bring independent evaluation. However, such trials are more complex in terms of coordination [26]. Employing blockchain technology can facilitate management of multicenter clinical trials, improve transparency, traceability of the consents in clinical trials, quality and reliability of clinical trials' data, and therefore increase patient involvement and adherence to the treatment [27, 28]. Keeping track of all the actions of data-sharing can be used in order to evaluate a threat to infer more information about a patient, by combining anonymized

datasets that contain the information about the same patient, and estimate the potential risks of the patient's privacy [29].

## 4 Limitations of blockchain for healthcare

In this section, we analyze the limitations of the existing approaches, including some that have been already proposed in the related works.

*Limited availability of the data.* The data are required to be available from anywhere at any time, yet compliant with the access-control policies specified by the patient. At the same time, the access-control policies might be expressed differently at various locations and across different types of data. Therefore, it is a challenge, to define unified rules for the global reachability of the data. One issue with permissioned blockchains is that due to its (consortium-oriented) nature, it is likely to be impossible to make it global, i.e., create a single consortium with unified governance.

*Vulnerability of the immutable data.* While, from the medical perspective, it is of high importance to ensure the immutability of the healthcare data, it is not desirable to have all the data immutably stored on the blockchain, even if encrypted, due to the highly sensitive nature of such information. For example, advances in quantum computing can represent a threat to most of the worlds cryptographic infrastructures [30] in the future. Moreover, the availability of certain types of data may present unexpected side-effects, such as the decision to store genomics data on the blockchain can affect the patient's relatives. To this end, design of on- / off- chain data structures, interoperation mechanisms between the ledger and off-chain data storages, and privacy-preserving protocols are of high importance.

*Lack of guarantee of consistency of the distributed ledger at any point in time.* Blockchain technology cannot guarantee that every peer in a network has a valid (shared by the majority) state. The peer may have an invalid state due to a software or hardware fault, or malicious attacks. Yet, the peer may still participate in the network albeit having an intermittent or permanent failure. Thus, it is important to ensure that the client (user) obtains valid information from the blockchain even in case of the presence of faulty nodes. Policy and additional mechanisms for querying the blockchain nodes are required in order to ensure obtaining and interpreting reliable answers from the blockchain.

*Introduction of a single point of failure.* In case of employing off-chain data storage (either for data storage or for running computations over the healthcare data) and membership service (in case of permissioned blockchain), the risk of creating a single point of failure exists. To mitigate this limitation the following approaches can be employed: applying cryptographic techniques (including symmetric and asymmetric encryption, digital signature, threshold encryption, and homomorphic encryption), decentralization of the data-storage and membership service, and involving trustful independent parties [10, 23, 31].

*Capabilities of current blockchain technologies.* Requirements from the healthcare perspective may not be easily satisfied by applying the technology "out-

of-the-box". Thus, bridging the gap between practical needs and technology capabilities may be required. Distributed ledger technology is developing fast, yet multiple limitations have been already identified by the research community, including the limited number of transactions that can be processed, limited data storage capabilities, concerns related to the immutability of the distributed ledger, the legal requirements of allowing opt-outs of data, and the need for standardization.

*Verification of the correctness of the smart-contract.* Design and verification of the smart-contract business logic cannot be performed in a fully automatic manner, and thus a human must be involved. This person is required to have both expert domain knowledge, as well as technical competence (i.e., one has to make sure that the rules are defined according to the use-case scenario). Moreover, verification of the correctness of the smart-contract implementation is of high importance to guarantee all mandatory tenets.

## 5 Research agenda for blockchain-based intelligent healthcare data management

In an attempt to bridge the gap between the listed domain-specific requirements and current technology implementations, while taking into account the analysis of the existing approaches and their limitations, we propose the following research agenda in the area of applying blockchain technology for intelligent healthcare data management. We present it in the form of research objectives (RO) encompassing technical, social, and legal aspects.

***RO-1:*** *Ensure privacy-preserving distributed and globally-reachable data.* The challenge of ensuring globally reachable data and enforcement of patient's access control policy is not trivial: data availability and interoperability requirements can interfere with the patient's privacy. Is it possible to define a harmonized and standardized set of basic rules that can be built into the healthcare data management architecture based on the international laws and regulations, preserving different sensitivity levels of the data, and ensuring adherence to such rules without a centralized authority?

***RO-2:*** *Ensure truthfulness of the data.* Blockchain is not concerned with truthfulness; it guarantees the immutability of data once recorded, regardless of the content. To ensure data quality, in permissioned blockchains, different approaches for the authentication of the users, the data providers, can be applied. One can employ cryptographic primitives (hash/digital signature) and store the output on the blockchain to ensure the immutability of the data that are stored off-chain. To establish the truthfulness, multiple independent oracles, or verifiers, can be involved (i. e., the data are considered genuine only after being approved by multiple parties). There exist some technology solutions, that can be directly paired with blockchain (e.g., IBM verifier [32]).

***RO-3:*** *Enable intelligent data-management.* How to design privacy-preserving hybrid data storage for machine learning tasks and artificial intelligence techniques (e.g., to use on-chain storage only for the statistical data avoiding storage

of sensitive data on the blockchain)? Can we decouple the query from the execution by defining the queries and parameters to be stored on the blockchain, which will be then executed only by trusted entities or data owners (doctors, patients)?

***RO-4:*** *Attain multi-ledger interoperability.* A plethora of existing blockchain platforms and various prototypes built on top of the technologies can aggravate the problem of the lack of interoperability between healthcare systems. Thus, ensuring interoperability between different blockchain platforms is of high importance. Moreover, due to custom privacy requirements and individual needs of different patients, one can think of a multiple-ledger design: a patient-specific, or even a case-specific ledger [33]. Data then can be replicated among multiple ledgers and locations, creating the network of networks [34]. Depending on the context, different requirements to access the data will have to be fulfilled. However, it is still unclear how patients will be able to manage their ledgers, as well as how to set up such infrastructure in real-world settings.

***RO-5:*** *Educate and involve the patients.* Before patients have full control over their data, the patients must be informed and educated about data- and consent- management practices as well as about existing laws and regulations.

***RO-6:*** *Assist patient with data-sharing decisions.* How to ensure that all the necessary data are shared in case of treatment of a specific condition? Smart systems for data-sharing decision making, which are based on ethics, law, and contextual medical requirements, are needed to guide and yet not to overwhelm someone already occupied with his/her treatment. These systems will be extremely useful for both primary care and secondary use of healthcare data, therefore advancing personalized medicine, and facilitating better treatment.

***RO-7:*** *Guarantee emergency data access.* In the healthcare domain, emergency situations, urgently requiring healthcare data, occur regularly. An access-control policy can be defined such that only the patient can access (is authorized to access) his data, and no caregiver from the medical institution (where the patient was delivered in an emergency situation) has permission to access any data about the patient. In the case when the patient is unconscious, it is impossible to grant access to the data to the caregiver. Robust and secure "break-glass" mechanisms for emergency situations are therefore required to address this limitation.

***RO-8:*** *Enable data analysis and research.* Having a complete, curated and trusted data set is critical for ensuring accurate results in analysis and research. For example, once complete and accurate data of oncology patients history are systematically stored with the use of blockchain with consent from the patients, the data can be leveraged in advancing oncology research and treatment options. Currently, analytical, compliance and research tools are actively researched and developed [6]. These tools will extend analytical and treatment capabilities; for example, having a detailed history of drug tolerance and side-effects on patients combined with their genetic profiles or markers can help to improve the selection of patient treatment options.

## 6 Conclusion

Blockchain technology increasingly attracts attention in multiple healthcare-related contexts, includig patient-centric data management, pharmaceutical supply-chain processes or medical research. Blockchain "promises" to address various inefficiencies of healthcare-related processes, by enabling better traceability, transparency, and efficiency. However, existing blockchain platforms can offer only limited capabilities and solutions from technical, legal, and social perspectives. The technology is in the early phases of evolution and development, yet, variety of platforms and their applications in healthcare settings already exist. This leads to the following paradox: recent attempts to address interoperability between different healthcare stakeholders already resulted in the creation of multiple blockchain-based prototypes built on top of different blockchain platforms, which themselves are incapable of seamless data exchange and integration. Moreover, due to some of the fundamental properties of blockchain technology (such as immutability), ensuring compliance with existing laws and regulations is challenging.

Starting from the healthcare context-based requirements, basic principles of the blockchain technology, and focusing on processes that can benefit from applying blockchain, we analyzed existing approached and listed their limitations. Based on this analysis, and taking into account the healthcare requirements, we emphasize the need for further research directions to be followed towards attaining blockchain-based intelligent healthcare data-management.

## References

1. "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA," http://data.europa.eu/eli/dir/2016/680/oj, last accessed 2019-05-05.
2. "Health Information Privacy U.S. Department of Health  Human Services," http://www.hhs.gov/hipaa/, last accessed 2019-04-05.
3. "Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research through 2024," "https://www.healthit.gov/sites/default/files/onc_pghd_final_white_paper.pdf, last accessed 2019-04-05.
4. "Draft Trusted Exchange Framework 2018," https://www.healthit.gov/sites/default/files/draft-trusted-exchange-framework.pdf, last accessed 2019-05-05.
5. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 2016, pp. 25–30.
6. D. Dillenberger, P. Novotny, Q. Zhang, P. Jayachandran, H. Gupta, S. Mehta, S. Hans, S. Chakraborty, M. Walli, J. Thomas *et al.*, "Blockchain analytics and artificial intelligence," *IBM Journal of Research and Development*, 2019.

7. M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, 2018.
8. A. A. Vazirani, O. ODonoghue, D. Brindley, and E. Meinert, "Implementing blockchains for efficient health care: Systematic review," *Journal of medical Internet research*, vol. 21, no. 2, 2019.
9. P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "Fhirchain: applying blockchain to securely and scalably share clinical data," *Computational and structural biotechnology journal*, vol. 16, pp. 267–278, 2018.
10. A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *AMIA Annual Symposium Proceedings*, vol. 2017. American Medical Informatics Association, 2017, p. 650.
11. I. Haq and O. M. Esuka, "Blockchain technology in pharmaceutical industry to prevent counterfeit drugs," *International Journal of Computer Applications*, vol. 975, p. 8887, 2018.
12. N. Hackius and M. Petersen, "Blockchain in logistics and supply chain: trick or treat?" in *Proceedings of the Hamburg International Conference of Logistics (HICL)*. epubli, 2017, pp. 3–18.
13. T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain," in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*. IEEE, 2017, pp. 772–777.
14. M. Bishop, *Computer security: art and science*. Addison-Wesley Professional, 2003.
15. Y. Sattarova Feruza and T.-h. Kim, "It security review: Privacy, protection, access control, assurance and system security," *International journal of multimedia and ubiquitous engineering*, vol. 2, no. 2, pp. 17–32, 2007.
16. S. De Lusignan, S.-T. Liaw, P. Krause, V. Curcin, M. T. Vicente, G. Michalakidis, L. Agreus, P. Leysen, N. Shaw, and K. Mendis, "Key concepts to assess the readiness of data for international research: Data quality, lineage and provenance, extraction and processing errors, traceability, and curation," *Yearbook of medical informatics*, vol. 20, no. 01, pp. 112–120, 2011.
17. S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.
18. Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in *International Conference on Financial Cryptography and Data Security*. Springer, 2015, pp. 507–527.
19. T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.
20. R. Krawiec, D. Housman, M. White, M. Filipova, F. Quarre, D. Barr, A. Nesbitt, K. Fedosova, J. Killmeyer, A. Israel *et al.*, "Blockchain: Opportunities for health care," in *Proc. NIST Workshop Blockchain Healthcare*, 2016, pp. 1–16.
21. S. Attili, S. Ladwa, U. Sharma, and A. Trenkle, "Blockchain: the chain of trust and its potential to transform healthcare–our point of view," in *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, 2016.
22. A. W. Peters, B. M. Till, J. G. Meara, and S. Afshar, "Blockchain technology in health care: A primer for surgeons," *Bulletin of the American College of Surgeons*, vol. 12, pp. 1–5, 2017.

23. G. Magyar, "Blockchain: Solving the privacy and research availability tradeoff for ehr data: A new disruptive technology in health data management," in *2017 IEEE 30th Neumann Colloquium (NC)*. IEEE, 2017, pp. 000 135–000 140.
24. K. A. Clauson, E. A. Breeden, C. Davidson, and T. K. Mackey, "Leveraging blockchain technology to enhance supply chain management in healthcare," *Blockchain in Healthcare Today*, 2018.
25. T. Scott, A. L. Post, J. Quick, and S. Rafiqi, "Evaluating feasibility of blockchain application for dscsa compliance," *SMU Data Science Review*, vol. 1, no. 2, p. 4, 2018.
26. L. M. Friedman, C. Furberg, D. L. DeMets, D. M. Reboussin, C. B. Granger *et al.*, *Fundamentals of clinical trials*. Springer, 2010, vol. 4.
27. A. Dubovitskaya, D. Calvaresi, and M. I. Schumacher, "Essais cliniques multicentriques: transparence et contrôle de la qualité grâce à la blockchain et aux systèmes multi-agents," *Swiss Medical Informatics*, vol. 34, no. 00, 2018.
28. A. Andrianov and B. Kaganov, "Blockchain in clinical trialsthe ultimate data notary," *Applied Clinical Trials*, p. 16, 2018.
29. M. Dumas, R. Hull, J. Mendling, and I. Weber, "Blockchain technology for collaborative information systems (dagstuhl seminar 18332)." Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019.
30. M. Mosca, M. Roetteler, N. Sendrier, and R. Steinwandt, "Quantum cryptanalysis (dagstuhl seminar 15371)," in *Dagstuhl Reports*, vol. 5, no. 9. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016.
31. Z. Shae and J. Tsai, "Transform blockchain into distributed parallel computing architecture for precision medicine," in *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2018, pp. 1290–1299.
32. V. Balagurusamy, C. Cabral, S. Coomaraswami, E. Delamarche, D. Dillenberger, G. Dittmann, D. Friedman, O. Gke, N. Hinds, J. Jelitto, A. Kind, A. Dinesh Kumar, F. Libsch, J. Ligman, S. Munetoh, C. Narayanaswami, A. Narendra, A. Paidimarri, M. Prada Delgado, J. Rayfield, C. Subramanian, and R. Vaculin, "Crypto anchors," *IBM Journal of Research and Development*, pp. 1–1, 2019.
33. A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "How blockchain could empower ehealth: An application for radiation oncology," in *VLDB Workshop on Data Management and Analytics for Medicine and Healthcare*. Springer, 2017, pp. 3–6.
34. T. Hardjono, A. Lipton, and A. Pentland, "Towards a design philosophy for interoperable blockchain systems," *arXiv preprint arXiv:1805.05934*, 2018.