JAMIA Open, 5(3), 2022, 1–8
https://doi.org/10.1093/jamiaopen/ooac068
Review

Review

Electronic health records and blockchain interoperability requirements: a scoping review

Suzanna Schmeelk [1,3] Megha Kanabar [1] Kevin Peterson [2], and Jyotishman Pathak [1]

[1]Department of Population Health Sciences, Weill Cornell Medicine, New York, New York, USA, [2]Center for Digital Health, Mayo Clinic, Rochester, Minnesota, USA, and [3]Director M.S. Cyber & Information Security Program, St. John's University, New York, New York, USA

Corresponding Author: Suzanna Schmeelk, DPS, EdD, MBA, MS, MS, MS, MS, MS, BS, Department of Population Health Science, Weill Cornell Medical College, Weill Cornell Medicine, New York, NY 10065, USA; sus4003@alumni.weill.cornell.edu

Received 18 February 2022; Revised 30 June 2022; Editorial Decision 5 July 2022; Accepted 20 July 2022

ABSTRACT

Objective: The purpose of this study was to conduct a scoping review of publications that explored blockchain technology in the context of interoperability and challenges of electronic health record (EHR) implementations. We synthesize the literature regarding standards and security, specifically regulation, regulatory operability, and conformance to standards. We review open practitioner questions that were not addressed in the studies as directions for further research.

Materials and Methods: We conducted a literature search in the OVID databases (Medline and Embase) on terms *blockchain*, *implementation*, *interoperability*, *EHRs*, *security*, and *standards*. The search resulted in 152 nonduplicate, peer-reviewed manuscripts, of which 15 were relevant to our objective and included for synthesis.

Results: Based on the search results, we analyzed the adoption of blockchain technology in the healthcare systems and challenges to EHR implementation of blockchain. From the synthesized research, we categorized and reported compelling factors of blockchain for EHR integration using current knowledge on blockchain research standardization and architectural challenges.

Discussion: Our research showed promise in implementing blockchain technology associated with EHRs, especially with Health Information Exchanges. The studies relevant for both EHR ($n=5$) and blockchain ($n=10$) reported compelling factors and limitations of the architecture. Security ($n=4$) and interoperability ($n=4$) features were reported as compelling requirements with lingering challenges. Standardization literature ($n=3$) reported implementation challenges.

Conclusion: This study shows promise in implementing blockchain technology within EHR systems. The adoption is increasing; however, multiple implementation challenges remain from architectural perspectives (eg, scalability and performance), to security challenges (eg, legal requirements), and standard perspectives including patient-matching problems.

Key words: blockchain, standards, interoperability, electronic health records

LAY SUMMARY

Blockchain technology has been adopted by industry due in part to its decentralized architecture, record fidelity, security features, and scalable design. In this scoping review article, we synthesize blockchain technology publications in the context of electronic health records (EHRs) implementations. We analyze the literature in terms of standards, security, and regulatory interoperability finding that some implementation challenges remain. We examined open practitioner questions that were not addressed in the studies as directions for future work. Overall the research finds promise in implementing EHR-specific blockchain technologies particularly with respect to Health Information Exchange integrations.

OBJECTIVE

Electronic health records (EHRs) contain identifiable, personal patient healthcare information. It is therefore essential to ensure secure interoperability within a hospital system. Recently, a new technology called *blockchain*, previously used in the financial sector, has emerged to potentially significantly improve secure data interoperability in the healthcare sector. Our scoping review investigates the opportunities, challenges, and open questions in the adoption and integration of blockchain technology within EHR systems. Our scoping review is synthesized and analyzed for responses to open healthcare sector practitioner questions. The open discussion questions are guided by insights from the paper authors' experience working with healthcare systems; these questions were not addressed in the literature either partially or fully. The aim of the open questions is to provide directions for research.

BACKGROUND AND SIGNIFICANCE

Blockchain is a peer-to-peer (P2P)-distributed ledger technology, developed in 2008, that requires validation from originators and organizers before being accepted.[1,2] It is a newer technology that has potential to significantly improve the data exchange in the healthcare sector,[3] especially during the sudden development of the COVID-19 pandemic, which has exposed some limitations in healthcare systems to handle public health emergencies.[4] By using a unique immutable architecture, blockchain can support characteristics of decentralization, exchange, anonymity, and accessibility. Examples can be found in finance,[5] radiology,[6] supply chain management,[7] and government,[8,9] among other[10] venues. A major strength of blockchain is its related and supportive cryptographic and distributed architecture for sharing meta-information or specific components of EHRs, while maintaining a high degree of transfer accountability and providing data exchange interoperability among healthcare entities.[11,12]

EHRs are being widely adopted by health systems and healthcare providers. Since EHRs contain identifiable and private patient information, data transfers between health systems and healthcare providers require a secure platform for exchange; hence, data sharing across disparate EHR systems remains a challenge. Blockchain could be a solution to enable secure data sharing. The overall objective of this scoping review was to determine if blockchain can improve interoperability and secure repetitive processes for efficient sharing and viewing of EHRs.

Current blockchain implementations (eg, Ethereum,[13] Bitcoin[14]) show promise in enabling information exchange, as the technology is a P2P, immutable, decentralized, and anonymous ledger, which can promote more efficient data sharing between entities (Figure 1). These key characteristics are very important for blockchain implementation in health care. Decentralization requires that information entered in the system must be accepted by all participating parties. There is also not one single authority that controls the addition of information onto the chain; instead, consensus must be met. These aspects of the historical blockchain architecture have the potential to reduce associated input centralization costs, as no mediator is required.[15] Another characteristic of the blockchain technology architecture is anonymity. Anonymity promotes a degree of privacy and security for healthcare records, while accessibility shows promise in the healthcare setting, as entries cannot be deleted after being chained.[16] These historical characteristics of the blockchain architecture make it compelling for healthcare sector implementation.

Notably, according to Hussien et al,[17] blockchain has four specific features that can be applied to the healthcare system: decentralized storage, consensus controls, immutability, and increased capacity. Blockchain can store information, deliver it to others upon the consent of the originator, and has features that only allow changes to the system when all parties are in agreement or consensus has been met. In addition, it is immutable meaning that data cannot be altered once it is accepted onto the chain. Finally, data are traditionally referenced from the chain rather than stored directly. Thus, blockchain is able to be written once and viewed many times; however, it cannot be modified once written, making it ideal in healthcare settings.

Furthermore, Vazirani et al[18] note that blockchain can effectively manage data, specifically EHR data, in healthcare. The authors also note "a Blockchain allows data across multiple independent systems to be accessed simultaneously and immediately by those with sufficient permissions." This has the potential to efficiently reduce administrative tasks of transferring data to other facilities ultimately with a trajectory to improve patient health. Efficient transfer of life-impacting patient data could encourage providers to focus their resources on patients while reducing needed resources related to EHR transfer verification and technical Open System Interconnect model exchange.[16]

MATERIALS AND METHODS

Literature search strategy

We developed a study protocol in compliance with the Preferred Reporting Items for Systematic Reviews and Meta-Analyses guide-

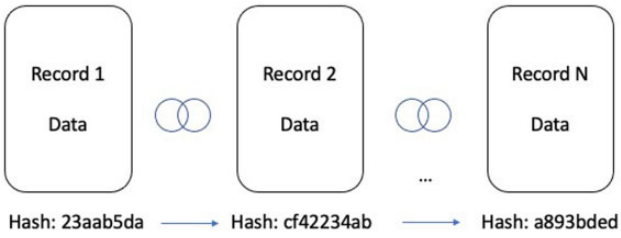

Figure 1. Blockchain implementation.

lines. Eligibility criteria for publications were (1) original research articles and systematic reviews published in peer-reviewed journals or conference proceedings; (2) reported findings from research that developed or employed EHRs and blockchain or focused on blockchain record security; and (3) written in English. We excluded articles that (1) were for blockchain implementations not specific to EHRs or were not covering open questions on blockchain record security for EHR-similar architectures, (2) duplicates, or (3) were for another non-EHR-specific systematic review.

Literature screening and selection

Based on Medical Subject Headings and literature browsing, we identified five groups of search terms to retrieve an exhaustive collection of relevant articles meeting the eligibility criteria summarized in Table 1: (1) blockchain; (2) interoperability, health information exchange; (3) EHR; (4) security, implications, challenges; and (5) standards, Health Level Seven (HL7).

We searched the OVID electronic search engine databases (Medline and Embase). The last search was run on April 25, 2021. Two members of the study team screened the titles and abstracts of the retrieved articles to evaluate their relevance to the present review. When an article's relevance could not be determined by its title and abstract, the full text was reviewed by the two reviewers based on the exclusion criteria.

Analysis framework

Overall, relevant articles were recorded on a data extraction form based on themes regarding the use of blockchain to achieve interoperability. The categories included: blockchain background, EHRs, interoperability, security to protect the patient information and organizational information systems from harm, and standards to enable data exchange among different technological components within and between organizations. Covidence® was used for each round to record study exclusions and reviews. Two review authors (SS and MK) independently screened the titles and abstracts against the inclusion criteria and repeated the process following full-text retrieval. Any screening disagreements were resolved by discussion, or reference to a third author (KP and JP). A list of studies excluded at the screening stage was recorded.

RESULTS

Our search yielded 281 publications. After the first review round where duplicates ($n = 129$) were removed, 152 unique publications were identified for the second review round. In the second review round, papers were excluded ($n = 92$) based on the exclusion criteria on the titles and abstracts alone. The third review round consisted of screening the full text of the articles ($n = 60$) identified from the prior round. In round 3, the full text was excluded ($n = 45$) based on the same exclusion criteria from the prior round applied on the full text. For the study inclusion, 15 articles were identified as eligible for data extraction and synthesis (Figure 2). The research synthesis is reported in subsequent subsections.

Table 1. Study inclusion results for EHR blockchain data synthesis

Keywords	Number of articles/[ID]
Blockchain	10[1,2,4,11,16,17,19–22]
Interoperability, health information exchange	4[1,2,11,17]
Electronic health record, EHR	5[1,4,17,20,21]
Security, implications, challenges	4[2,21,23,24]
Standards, Health Level Seven, HL7	3[12,18,19]

EHR: electronic health record; HL7: Health Level Seven.

Blockchain and EHR integration

Dubovitskaya et al[1] analyzed EHR data sharing using blockchain introducing a novel framework for managing and sharing EMR data for cancer patient care. The authors report that EHRs are electronic, therefore easier to potentially share between healthcare entities such as pharmacies, insurance companies, patients' families, and other healthcare providers. One example use case for EMR blockchain included primary patient care, which would solve the problem of patients not having their records when moving from hospital to hospital. Another blockchain use case envisioned data aggregation for research since patients are often unwilling to participate in data sharing across organizations due to the current lack of appropriate data sharing mechanisms and distributed coordination efforts such as signing and sending consent forms to different entities. The authors suggested that blockchain may ultimately assist in connecting different healthcare systems for improved patient care. The authors proposed a novel framework on managing and sharing EHR data for cancer patient care. They implemented the framework as a prototype in collaboration with Stony Brook University reporting on their experiences. The prototype was developed to provide a chain for sharing data between oncology patients and their doctors, specifically patient history and physical exams, laboratory results, and delivered radiation doses. The chain was a solution developed to improve assurance that shared patient data are fast and convenient while complete, securely stored, and accessible only according to the patient's consent.

Mayer et al[4] systematically synthesized 38 studies from the last decade of scholarly research on EHR in blockchains. Their research and synthesis included novel questions for EHRs in a blockchain for building a blockchain taxonomy; examining known challenges; important principles, protocols, standards, and open questions; analyzing architectures; and discussions on long-term blockchain needs for the "ever-growing" storage of patient medical records. Their synthesis identified and summarized high-level relevance of blockchain categories and underlying-terms within security, scalability, governance, interoperability, and privacy while noting which papers discussed the topics. Our research differs from research of Mayer et al and other similar reviews, in that we explore blockchain literature with different inclusion criteria and previously unpublished open practitioner questions regarding blockchain.

Blockchain and interoperability

Interoperability is defined by the Health Information and Management Systems Society as "the ability of different information technology systems and software applications to communicate, exchange data, and use the information that has been exchanged.[20]"

Gordon and Catalini[20] explore blockchains to facilitate interoperability, which they report has many benefits. One interoperability benefit is that well-communicating systems can improve efficiency and reduce time spent on forwarding patient records to other facilities. Another benefit from a properly architected blockchain system is that by sharing data on the chain can reduce duplicate clinical interventions for a patient potentially improving their safety. The authors predict that blockchain can improve patient-driven interoperability through five methods: data access, data aggregation, data

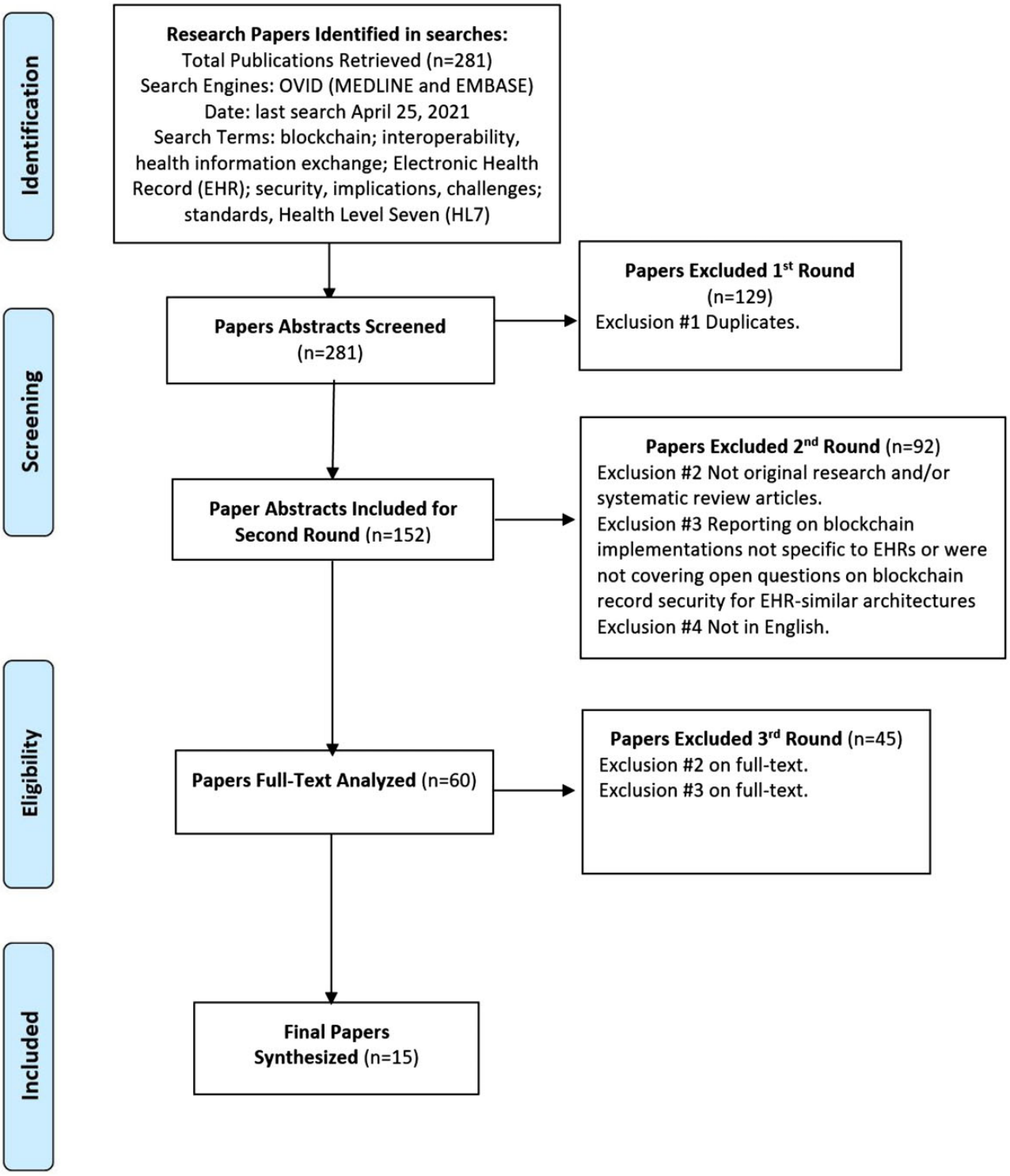

Figure 2. Research inclusion PRISMA. PRISMA: Preferred Reporting Items for Systematic Reviews and Meta-Analyses.

liquidity, patient identity, and data immutability. Developing such a unique patient identifier comes with new security risks.

In another study, Yan et al[25] explain the key challenges in traditional Health Information Exchange (HIE) and relate them to blockchain solutions. The first challenge they analyze is the potential data inconsistency concerns due to transmission loss, which can be solved once on the chain, due to the chain's immutability feature. Another historical HIE challenge has been security and privacy concerns due to unauthorized access. Blockchain may improve such mitigations from its immutable structure, perhaps through more accurate authorization. In addition, the traditional HIE problem of having multiple patient records for a single patient, at least at an institution, may be solved through building blockchain architectures with asymmetric key features for every participant. Such a feature could improve ac-

cess control and authorization but may come with other potential security and privacy risks.

In a similar study, Shaun et al[23] report that blockchain has the potential to improve accessibility, interoperability, and security of the healthcare system and EHRs. They report in their study that several blockchain verification processes exist ranging from public to private with varying levels of accessibility and governance; for example, implementations ranging from open blockchains, where anyone can interact, to private blockchains where permissions are required. The authors explain that despite the increasing adoption of EHRs, there still remains a barrier to robust information exchange. Blockchain integration with EHRs impacts every area of healthcare delivery: patients, providers, pharmaceuticals, industry, research, and government systems. At the patient level, the plethora of patient-generated data through mobile applications and other digital tools coupled with HIE blockchain can enable clinicians to have more accurate data to enable efficient and personalized care without redundant investigations. Other research and developer-based blockchains are reported to lead to faster time-to-market and cheaper products and services for both patients and providers. Overall, they concluded that blockchain is promising in HIE transparency, efficiency, and patient's safety and may encourage more robust medical research.

Challenges with blockchain implementation

To synthesize challenges with blockchain implementations in the areas of standards and security, we reviewed the research to develop a set of historical challenges in both domains. A major challenge in all areas related to the lifecycle of healthcare data, such as EHR contents, comes with major security regulation adherence and implications. For example, the European Union General Data Protection Regulation[26] requires that system users have the right to delete their data from a system. A blockchain architecture may not have been developed to support such a legal requirement with the ability to delete user or patient data. Similarly, blockchain, a newer technology, comes with such enhancements and challenges. With proper architectures, blockchain offers enhancements to privacy and security; however, scalability remains a current limitation. One scalability area that has seen recent success is in the area of standardization.

Standardization, such as efforts made by HL7, is enabling more effective data exchange, for example, by improving the reliability of semantic exchange. HL7 creates rules for structuring data to improve accurate dataflow between information systems. It includes a newer XML-based Fast Healthcare Interoperability Resources (FHIR) protocol which defines how healthcare information can be exchanged. Standardization, however, has interoperability limitations with legacy systems.

Overall, properly architected blockchain solutions have the potential to more efficiently and securely transfer life-critical data to ultimately improve the quality of life for many patients.

Standards

Anton et al[16] systematically reviewed, assessed, and synthesized 39 peer-reviewed full paper publications prior to October 2018. The analyzed papers proposed blockchain solutions to improve processes and services in healthcare, health sciences research, and healthcare education. Their research synthesis included types of blockchain (eg, public, private), platform/frameworks (eg, Ethereum, Hyperledger Fabric), usage of consensus algorithms, and the usage of smart contracts. The authors summarized their analysis by indicating their research article quality metric (eg, problem description, research objective) for each paper finding that the average quality score of the blockchain research per year from 2016 to 2018 was trending upwards. The authors noted that further research should address challenges of how blockchain-based solutions can be made to comply with current health data laws and standards.

In another study, Peng et al[12] provided contributions for applying blockchain technology to clinical data sharing in the context of technical requirements defined in the "Shared Nationwide Interoperability Roadmap" from the *Office of the National Coordinator for Health Information Technology* (ONC). They analyzed the national requirements and their implications for blockchain-based systems; and then, proposed a novel blockchain, *FHIRChain*, designed to meet ONC requirements by encapsulating the HL7 FHIR standard for shared clinical data. The proposed application was a decentralized application using digital health identities to authenticate participants in a case study of collaborative decision making for remote cancer care. The research identified five architecture requirements: (1) verifying identity and authenticating all participants, (2) storing and exchanging data securely, (3) consistent permissioned access to data sources, (4) applying consistent data formats, and (5) maintaining modularity. The authors note that in practice, many barriers exist in current technical infrastructures of health IT systems today including privacy/security concerns, scalability concerns, and healthcare entities trust concerns, and the lack of interoperable data standards enforcements. Lastly, the case study identified limitations to be addressed in future blockchain research: semantic interoperability, legacy system compatibility, inability to directly control clinical malpractice, and deployment costs.

Security

Poobalan et al[24] developed a novel framework on privacy preservation of electronic health records using blockchain technology. Their analysis of the developed framework was qualitative and quantitative in traditional challenge areas of efficiency, storage, security, and scalability. The authors compared their approach with other blockchain implementation designs in terms of the traditional challenges of data integrity, data privacy, data security, confidentiality, and scalability. The analysis found that most current blockchain architecture research accommodates higher degrees of certain data integrity and data confidentiality areas, but challenges remain for other privacy, security, and scalability concerns.

Houshyar et al[21] found that a lack of a comprehensive standard architecture, cloud server availability, capacity, susceptibility to manipulation, scalability, and cost limitations remain critical challenges with the blockchain technology implementation. Similarly, Matheu et al[2] described an approach to enforce security restrictions during the device bootstrapping process, again speaking to the overall blockchain architecture security.

Shaun et al[23] reviewed the case of employing blockchains for EHRs. The authors note advantages such as public-key cryptography, accessibility, transparency, accuracy, efficiency, utility, and interoperability characteristic of blockchain, which make it a compelling solution. The authors also note historical blockchain challenges, such as data throughput speed, file type/size restrictions, and data security. The authors bring forward regulatory and institutional challenges. For example, regulatory challenges encompass local, national, and international legal and industry requirements. Institutional challenges encompass actual blockchain implementation tools and end-user usage motivation. Overall, the authors find

that blockchain holds promise for augmenting HIEs, improving data transparency, improving the safety of patient care, improving healthcare efficiency, and more robust medical research.

DISCUSSION

This scoping review revealed that blockchain may provide seamless exchange of private patient data using a secure method. Blockchain's inherent characteristics (eg, decentralization, accessibility, and anonymity, as listed by Hasselgren et al[16]) show that EHRs may be safely transferred among health systems and healthcare providers. In addition, properly architected blockchain implementations could save provider time, allowing them to spend their time directly tending to their patients instead of administrative duties. Further full-lifecycle research needs to be addressed, as reported by Matheu et al.[2]

However, there are also significant limitations in wide-scale adoption of blockchain technology. McDonald's article[22] reports on very early concerns of standards and security of EHR implementation. These historical concerns remain similar to the concerns that are currently manifested in implementing blockchains. Historically, the first step of transferring data from pen and paper records to electronic records was executed fully in 2009 to the usage of 96% of nonfederal acute care hospitals using EHR in 2015.[20] Currently, blockchain implementations may allow for better interoperability of patients' information. The dream is the ability of patients to seamlessly shift institutions in search of the best possible healthcare.

Data, emphasized by Zhuang et al,[25] should only be accessible by authorized entities. One way to approach data sharing authorization is by employing asymmetric cryptography keys to entities that need to authorized transactions; such entities include patients and their healthcare workers. With enabled architectures, keys could be constructed between participating institutions to eliminate patient-matching concerns. Mehta et al,[23] project that this could enable more robust patient care by reducing administrative tasks.

Further research needs to develop HL7 interoperability requirements for EHR Blockchain implementations. Some general HL7 considerations, reported by Tuncay et al[27] include developing interoperability test frameworks for systems conforming to HL7 requirements. Specifically, the authors identified the following requirements: (1) testing interoperability of the messaging interface with different standards and protocols; (2) evaluating interfaces for document interoperability, syntactic validation, and semantic verification of HL7 messages and documents; (3) testing the design and management Graphical User Interfaces; and (4) building a test framework database. The researchers identified that conformance and interoperability testing are essential for maintaining correct HIE as interoperability standards often contain certain ambiguity in their specifications that may result in differences in their implementations.

Standards, such as HL7 FHIR, achieve national HIE requirements. Reported historical challenges to standards remain semantic interpretation and legacy system interoperability. Blockchain EHR security strengths are reported to include data integrity and confidentiality. For example, integrity is inherent when audit trails are created. And, data confidentiality can be protected by architecting the chain so that sensitive information is not revealed. Research reports that blockchain scalability, privacy, lifecycle, and security are more difficult problems (Table 2).

Open questions remain from the authors of this paper as practitioners and researchers in the healthcare sector field as we were unable to identify closely related discussions in the reviewed literature. Table 3 (appendix) synthesizes remaining questions to guide future research.

Limitations

This research is limited to studies related to EHRs and Blockchain and does not include other Blockchain applications in the healthcare field, for example, radiology reports and pharmacy applications. The keywords used in this study were a list of keywords and did not include all permutations of the words (eg, EMR instead of EHR); hence, the results of this study may not include all related publications. The review also focused solely on articles related to EHRs and Blockchains.

Future work

Future work includes collecting additional analytics on blockchain implementation successes in healthcare settings as blockchain case studies begin multiyear deployment. With longer running case studies and the introduction of newer novel architectures, additional studies could examine more up-to-date analytics, additional data components, and different system architectural designs. For example, collecting institutional review board-approved interviews with healthcare practitioners supporting different job functionalities could produce a comprehensive set of open practitioner questions. Furthermore, as all deployed technology likely leads to data breaches or other adverse challenges with time, future work should analyze adversarial attacks or related challenges to deployment over time.

As some proposed novel blockchain EHR architectures involve institutional-dependent creations of user keys during enrollment and will likely run into patient identification problems (eg, Benson et al[19]) with needed areas for future work.

Table 2. Findings synthesis of blockchain EHRs, security, and standards

Topic	Compelling features	Architectural challenges	References
Blockchain EHRs	Accuracy, accountability, security, privacy, accessibility, access control, transparency, efficiency, utility, interoperability	Speed, file size, file type limitations, regulatory data security concerns, stability, robustness	10[1,2,4,11,16,17,19–22]
Security	Cryptography, auditing, data providence	Scalability, privacy, access control	4[15,19,23,24]
Standardization	ONC regulatory interoperability, conformance to existing standards	Regulatory, institutional, legacy systems, semantic, patient matching	3[12,18,19]

EHRs: electronic health records; ONC: Office of the National Coordinator for Health Information Technology.

Table 3. Synthesis of open practitioner questions for blockchain implementations

Topic	Sub-topic	Remaining questions
Blockchain and interoperability	Identity	To have a distributed patient record, we must establish a consistent representation of patient identity. This is one of the largest challenges in this space. At the heart of this problem is who controls this identity. Is it the user themselves? Or is it some healthcare system or government organization that issues patients some identity key? How is that key associated with the actual person? Do they keep it on a smartphone for example? If so, what about patients that do not have a smartphone? Associating some digital "identity" to an actual person consistently is one of the main struggles with HIE in general, but with blockchain specifically.
Challenges with blockchain implementation	Scalability	Some of the heavily deployed consensus algorithms work on the condition that the network throughput needs to be slowed down. What is the effect on throughput and cost?
	Does the blockchain model fit?	Blockchain is essentially an implementation of sociology; if we can encode an incentivization model such that individuals are incentivized to reach correct and fair consensus, while bad actors cannot gain from cheating, then everything works. But historically such a model only works because of the incentives. Take Bitcoin, for example; if there was no incentive to mine, miners would not mine blocks and the consensus algorithm would not work. Now, in terms of healthcare, there are few, if any, research discussing incentive models. Why would hospitals put data on a blockchain? Who would drive consensus (and what would they get for doing so)? A key question is why is a blockchain better than a distributed database, for example? Or even a centralized database? What are potential incentives for the different models? What is the "value" in healthcare records? And, who "owns" them? Is an expensive imaging report "worth" the same as a blood pressure reading? These incentive models can get into really complex ethical questions.
	Trust	Trust is at the heart of the healthcare industry. Patients go to a hospital because they trust the clinicians and staff. Blockchain is designed to not require trust in individual actors. How are patients going to respond to this model? Would patients trust their healthcare record if it was stored on a blockchain vs. managed by their local hospital?
	Consensus algorithms	How is consensus built? Implementations are known to work, but they have been reported to be slow and energy consuming. There also needs to be some incentive to mine. Proof-of-stake gets around some of these challenges, but how do we define "stake" in healthcare?
Standards		HL7 FHIR has a promising use case. It also lends itself well to the "off-chain" use case (below). It would be useful to contrast some standards that are trying to align themselves with blockchain implementations.
Security	On vs. Off Chain	How does healthcare data actually get "stored" using a blockchain? You can put the data on the actual chain, but there are disadvantages to that—notably, that it is PHI going on a potentially public blockchain. It can be encrypted, but all encryption has a shelf life so "on-chain" storage is usually seen as not applicable for healthcare. "Off-chain" storage can be where the blockchain stores pointers or references to the actual data (which is then resolved later). This is usually seen as the most promising approach for healthcare.
	Public/private/permissioned?	A large challenge in healthcare is how to set up the blockchain. Should it be public/open (like Bitcoin, etc.)? Or should it be private or some sort of "permissioned" setup where only known parties are allowed to participate? Any healthcare data (even pointers and references) on a public blockchain is going to be almost universally a nonstarter, even with anonymity via encryption. Private or permissioned blockchains introduce the very thing blockchain was designed to avoid: individual trust. Who decides who is allowed in? Who maintains the list? It drives the implementation toward centralization.

FHIR: Fast Healthcare Interoperability Resources; HIE: Health Information Exchange; HL7: Health Level Seven; PHI: Patient Health Information.

CONCLUSION

Blockchain is a newer technology that is already being deployed in healthcare settings for many reasons. This scoping review synthesized blockchain EHR use cases and compelling architectural features and identified historical standards and security advantages and challenges. We identified areas for future research including historical health informatics challenges, such as proper semantic analysis of blockchain data transfer and potential patient-matching concerns. Overall, blockchain currently appears to be a compelling solution for HIE networks and ONC requirements. As deployed chains become longitudinal case studies, the healthcare industry will be able to identify and build proper solutions for all stakeholders.

FUNDING

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

AUTHOR CONTRIBUTIONS

All authors contributed to the design of the research. SS, MK, JP, and KP participated in the review as reported in the methodology.

CONFLICT OF INTEREST STATEMENT

JP reports being founder and an equity stakeholder at Iris OB Health, Inc. The other authors report no conflict of interest.

DATA AVAILABILITY

The data underlying this article will be shared on reasonable request to the corresponding author.

REFERENCES

1. Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and trustable electronic medical records sharing using blockchain. In: AMIA an-

nual symposium proceedings. Vol. 2017. American Medical Informatics Association; 2018: 650–9.
2. Matheu SN, Robles Enciso A, Molina Zarca A, *et al*. Security architecture for defining and enforcing security profiles in DLT/SDN-based IoT systems. *Sensors (Basel, Switzerland)* 2020; 20 (7): 1882.
3. Peterson KJ, Deeduvanu R, Kanjamala P, Mayo KB. *A Blockchain-Based Approach to Health Information Exchange Networks*; 2016. https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf.
4. Marbouh D, Abbasi T, Maasmi F, *et al*. Blockchain for COVID-19: review, opportunities, and a trusted tracking system. *Arab J Sci Eng* 2020; 45 (12): 9895–17.
5. Zaza T, Boudreau HS, Boyd CJ. The utilization of cryptocurrency as financial reimbursement in dermatology practices. *Dermatol Online J* 2021; 27 (10). doi: 10.5070/D3271055632.
6. Tagliafico AS, Campi C, Bianca B, *et al*. Blockchain in radiology research and clinical practice: current trends and future directions. *Radiol Med* 2022; 127 (4): 391–7.
7. Sharif A, Kumar R, Ouyang J, *et al*. Making assembly line in supply chain robust and secure using UHF RFID. *Sci Rep* 2021; 11 (1): 18041.
8. Lindman J, Berryhill J, Welby B, Piccinin-Barbieri M. The uncertain promise of blockchain for government. OECD Working Papers on Public Governance, No. 43. Paris: OECD Publishing; 2020. https://doi.org/10.1787/d031cd67-en.
9. Brinkmann M. The realities of blockchain-based new public governance: an explorative analysis of blockchain implementations in Europe. *Digit Gov Res Pract* 2021; 2 (3): Article 29.
10. Wei Q, Li B, Chang W, Jia Z, Shen Z, Shao Z. A survey of blockchain data management systems. *ACM Trans Embed Comput Syst* 2022; 21 (3): 1–28.
11. Abu-elezz I, Hassan A, Nazeemudeen A, *et al*. The benefits and threats of blockchain technology in healthcare: a scoping review. *Int J Med Inform* 2020; 142: 104246.
12. Zhang P, White J, Schmidt DC, *et al*. FHIRChain: applying blockchain to securely and scalably share clinical data. *Comput Struct Biotechnol J* 2018; 16: 267–78. 10.1016/j.csbj.2018.07.004.
13. Pustišek M, Umek A, Kos A. Approaching the communication constraints of ethereum-based decentralized applications. *Sensors (Basel, Switzerland)* 2019; 19 (11): 2647.
14. McGinn D, McIlwraith D, Guo Y. Towards open data blockchain analytics: a Bitcoin perspective. *R Soc Open Sci* 2018; 5 (8): 180298.
15. Vazirani AA, O'Donoghue O, Brindley D, *et al*. Implementing blockchains for efficient health care: systematic review. *J Med Internet Res* 2019; 21 (2): e12439.
16. Hasselgren A, Kralevska K, Gligoroski D, *et al*. Blockchain in healthcare and health sciences—a scoping review. *Int J Med Inform* 2020; 134: 104040.
17. Hussien HM, Yasin SM, Udzir SNI, *et al*. 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 (10): 1–35.
18. Vazirani AA, O'Donoghue O, Brindley D, *et al*. Blockchain vehicles for efficient medical record management. *NPJ Digit Med* 2020; 3 (1): 1–5.
19. Benson T. *Principles of Health Interoperability HL7 and SNOMED (1st ed. 2010. ed., Health Informatics)*. London: Imprint—Springer; 2010.
20. Gordon WJ, Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Comput Struct Biotechnol J* 2018; 16: 224–30.
21. Honar Pajooh H, Rashid M, Alam F, *et al*. Multi-layer blockchain-based security architecture for internet of things. *Sensors (Basel, Switzerland)* 2021; 21 (3): 772.
22. McDonald CJ. The barriers to electronic medical record systems and how to overcome them. *J Am Med Inform Assoc* 1997; 4 (3): 213–21.
23. Mehta S, Grant K, Ackery A, *et al*. Future of blockchain in healthcare: potential to improve the accessibility, security and interoperability of electronic health records. *BMJ Health Care Inform* 2020; 27 (3): e100217.
24. Poobalan A, Uma Maheswari N, Venkatesh R. Cloud computing security for electronic healthcare records using block-chain model. *Eur J Mol Clin Med* 2020; 7 (4): 2007–14.
25. Zhuang Y, Sheets LR, Chen Y-W, *et al*. A patient-centric health information exchange framework using blockchain technology. *IEEE J Biomed Health Inform* 2020; 24 (8): 2169–76.
26. General Data Protection Regulation (GDPR). *General Data Protection Regulation (GDPR)*; 2018. https://gdpr-info.eu.
27. Namli T, Aluc G, Dogac A, *et al*. An interoperability test framework for HL7-based systems. *IEEE Trans Inf Technol Biomed* 2009; 13 (3): 389–99. doi:10.1109/TITB.2009.2016086.