BLOCKCHAIN™ IN HEALTHCARE TODAY

Toward Application of Blockchain for Improved Health Records Management and Patient Care

Gracie Carter,[1] Denise White,[1] Anusha Nalla,[1] Hossain Shahriar,[2] Sweta Sneha[2]

Affiliations: [1]Masters of Science Healthcare Management and Informatics candidate, Kennesaw State University, Kennesaw, Georgia, U.S.A.;[2] Faculty Coles College of Business, Kennesaw State University, Kennesaw, Georgia, U.S.A.

Corresponding Author: Gracie Carter, Kennesaw State University, Kennesaw, GA, USA; gcarter7@students.kennesaw.edu

Keywords: Blockchain, EMR, Ethereum, Healthcare Information Technology, Patient Care, Records Management, Security, Smart Contract

Section: Systematic Reviews

Technological advancements have proven to be indispensable for improving patient care, yet they continue to present a host of problems. One of the most pressing concerns is how to improve quality of care while controlling costs. Beyond clinical care, one plausible solution is to share patient information freely and efficiently. Hospitals and clinics may share data internally, but external information sharing remains an issue. Despite the digitization of medical records, there remains a lack of adequate computing infrastructure or unwillingness to share data among providers. Care quality often suffers as a result. Implementing a type of peer-to-peer distributed digital technology, known as a blockchain, to record and transmit transactional data could be a solution to these concerns. Originally, blockchain was developed to record cryptocurrency transactions. However, as blockchain technologies have matured and adopted across dissimilar industries, the feasibility of possible applications of blockchain technology in healthcare is getting more attention. This article explores possible opportunities of adoption of blockchain technology to improve patient data security, privacy, and care while outlining the challenges that practitioners may encounter.

This article focuses on application of blockchain technologies to address issues in electronic health records and patient care, including cost savings, security, and fraud prevention.

Within the last decade, in the United States, there has been a technological revolution within the healthcare community through adoption of electronic health records (EHRs). Two bills were passed in 2009 that ushered in a new era in healthcare. The American Recovery and Reinvestment Act (ARRA) and, within ARRA,

the Health Information Technology for Economic and Clinical Health (HITECH) Act, were monumental for the advancement of healthcare. HITECH set aside nearly $27 billion over the course of 10 years[1,2,3] in incentives and set forth the Meaningful Use criteria, which focused on the optimization of electronic medical records (EMRs) through improved care quality, efficiency, and error prevention. In addition, providers were to digitize their medical records and implement EMRs through meaningful use or risk of losing their Medicaid and Medicare reimbursement.[1,2] The intention of Meaningful Use was to improve information exchanges among providers.[4]

HITECH mandated that the Office of the National Coordinator (ONC) for Health Information Technology should create an infrastructure for a nationwide health information exchange that allowed for the flow of health information electronically.[5] While EMRs streamlined records, the caveat was that these often were contained in a single health system.[5] Record transmittal to the next point of care was not always guaranteed without a reciprocity agreement in place.[6]

This breakdown in communication was one of the unforeseen shortcomings of the HITECH Act. However, the 21st Century Cures Act supported HITECH by defining and setting expectations for information sharing. A survey of health information exchange organizations revealed that more than 170 regional health information organizations did not met the criteria for the comprehensive health information exchange.[5]

Although HITECH proved effective in motivating the transition to EHRs, and the Cures Act mandated interoperability, there has been no system mandate nor was there any requirement for data sharing. A survey of health organizations revealed that more than 170 regional health organizations did not meet the criteria for the comprehensive health information exchange.[5] This cross-system information exchange is referred to as *interoperability*. The issue plaguing the healthcare community is how to seamlessly share these data.

Currently, EHR programs are a profitable business. For example, if a facility that chooses to use Epic's EHR wishes to modify or integrate features into their system, that facility must pay for the service,[7,8,9] as Epic maintains complete control over customization of their EHR program and charges to modify it.[8] Every healthcare facility or system has the freedom of choice with EHRs. Perhaps, it is the intersection of choice coupled with protectionist policies by EHR developers that make interoperability a difficult task.[8,9,10] This could have been avoided through a common data standard in conjunction with the HITECH Act.

As medicine rapidly advances, healthcare information technology (HIT) struggles to provide effective and affordable solutions to interoperability. Multiple resolutions are available to solve the issue of interoperability, but require cooperation of stakeholders. A functional and stable program that is lightweight, easy to operate, and relatively quick to implement might be met with less resistance and greater adoption by healthcare providers. Cloud-based data storage and sharing have promise, but questions of security limit desirability.[11,12,13]

Blockchain technology would bridge the communication gaps between disparate EHR systems.[2,9,14] It is more secure than cloud, no single entity controls information, and it is relatively simple to implement.[8]

BLOCKCHAIN

A blockchain is a distributed ledger or an unchangeable (immutable) record of transactions.

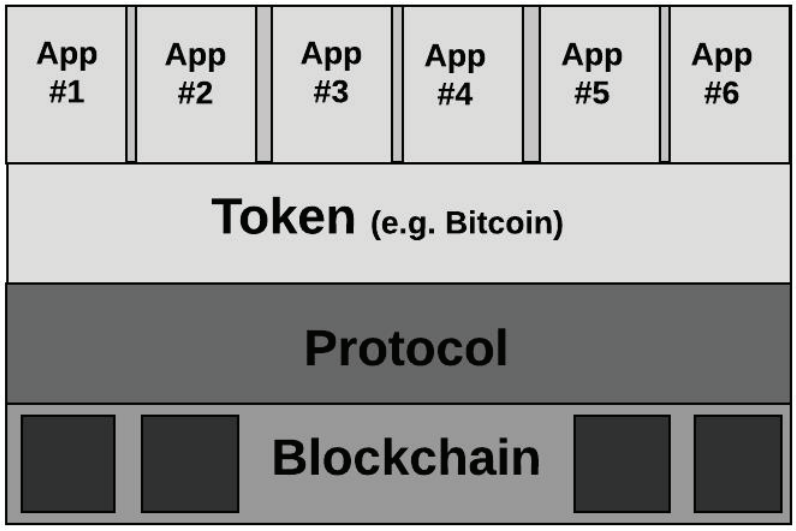

Figure 1.—Blockchain architecture.

Blockchain is a utility that other programs are built on (see Figure 1).

While there are many different models of blockchain and distributed ledgers available, this article will focus on Bitcoin,[15] Ethereum,[16] and Hyperledger.[16] These three models were chosen for their maturity level and popularity.

Bitcoin is the most mature blockchain platform. Bitcoin uses a public and permission-less distributed ledger. Hashes on blocks on the chain are verified through proof of work, a resource- and time-intensive consensus algorithm. To ensure security, the consensus of 51% of nodes is needed to verify a hash. Once a hash is verified, it is added to the chain and the original node is awarded a token. A token can be whatever the chain values, such as cryptocurrency. Each block is built on the preceding block and is added to the ledger, thus creating the blockchain.

The Ethereum chain is next most mature technology. The Ethereum chain is public and utilizes Ether as a token. Ethereum uses a proof-of-stake consensus protocol. In proof-of-stake, validators vote on proposed blocks based on the size of their stake in the chain. All Ethereum transactions utilize coding scripts to execute specified functions automatically. These are known as smart contracts.[16] The advent of smart contracts added immense value and versatility to the Ethereum chain.

Hyperledger is the last model of blockchain. It can be either a permissioned, private, or public blockchain. Hyperledger was developed by the Linux Foundation with input from respected industry leaders such as IBM and Intel,[16] and aimed at cross-ledger transactions. Hyperledger Fabric uses its own version of smart contracts known as chain code, but does not use a cryptocurrency as a token.[16] Hyperledger is becoming the blockchain of choice in healthcare due to versatility, configurable consensus protocol, and multiple offerings to suit consumer needs.

INTEROPERABILITY

Interoperability is the ability of two or more systems to share healthcare data for use by recipients.[10] Noninteroperability hinders cost

and quality of patient care. Without access to complete records to fully understand a patient's history, providers waste time and resources. According to the ONC for Health Information Technology, a functional system should include the following: a secure network infrastructure, verification of identity and authentication of all participants, and consistent proof of authorization of electronic health records.[5,17] However, no EHR was chosen nor a requirement for interoperability was mandated by the US federal government.

Because of legislation passed at the federal level with little strategic planning, healthcare providers at the local level adopted EHRs ad hoc to meet meaningful use. This lack of foresight coupled with a disinterest in active record management by patients has further complicated interoperability.[10]

If issues hindering interoperability were resolved, it could result in cost reductions[10] through allowing complete data to be accessed, thus improving clinical workflow.[18,19] In many care settings, patient records are only obtained through telecommunications by a doctor, nurse, or the patient.[15] Rather than spending the time looking for records, clinicians often reorder tests to save time![20] According to a survey conducted by KLAS Research, only 6% of clinicians found that information from other organizations was easy to obtain without interrupting their workflow, and fewer than one-third said they could access data from other EHRs easily.[15]

Noninteroperability makes utilizing new technologies difficult moving forward.[21] This is a direct result of market competition. Often, providers must join multiple networks with differing interfaces due to a lack of integration or cross-system communication.[20] This results in increased costs to maintain multiple vendor interfaces.

Blockchain is a viable alternative method for data sharing that offers a complete source of data. Currently, the foundational, structural, and semantic levels of interoperability are fraught with interpretation issues. The foundational level of interoperability is the most basic in which a cache of medical records is sent (pushed) from one provider to another.[15] It is assumed that the recipient of the data received it intact and can interpret it correctly.[15,18,22] There is no accountability with this method.[15] If the interfaces do not communicate through common data models, then the data are not usable. At the structural level, records are pulled between two systems where data structures are defined.[15,18,22] In this scenario, there is no audit trail between systems,[15,18,22] which allows for duplicate record requests and poses a security risk. At this level, the information is available, but not readily. Semantic is the highest level of interoperability. This would be the paramount model of effective communication. Providers would be able to view and pull the most accurate data without necessarily having an established relationship.[18,22]

Blockchain users would instantly achieve semantic interoperability. The data would be readily available for viewing using a distributed ledger. Healthcare providers could have coherent collaborative records without the cost of reconciling differing EHR interfaces.[15]

Blockchain could improve continuity of care by granting patients greater access to their own health records. Active involvement in the management of their healthcare data could encourage a healthier lifestyle through putting the patient at the center of their own care.[2,20] It would impart an unprecedented level of knowledge and power to the patient. Historically, patients were not able to revoke a provider's access to their records. Theoretically, a record was the possession of that provider permanently.[15,18]

This resulted in fragmentation of data and increased the chances of security breaches.[18] Blockchain puts the power of sharing squarely in the hands of the patient using permissions. This allows the patient, not the provider, to decide who had access to their data and when.[2,15,18] This concept is known as identity management.

Identity management places the patient at the center of their care. The primary tenet of patient-centered care is that all services are geared toward the requirements of the patient. Today, most healthcare workflows are geared toward the clinician.[23] Although it sounds elementary, patient-centered care is a no small task.

With the use of permissioned blockchains, entire records would not be stored in the chain due to current restrictions on block size. Instead, records could be accessed through metadata or through pointers to off-chain secure storage.[24] This would improve security and increase efficiency by eliminating the need to hunt for records. Efficency is becoming an important cost control measure, as healthcare costs account for 17.9% of the gross national product in the United States, and continues to rise.[3]

ENHANCED EHR SECURITY WITH BLOCKCHAIN

As EHRs were adopted, providers were suddenly inundated with digital data. To focus more on patients and less on data management, most facilities store patient health information in a cloud rather than in file rooms.[25] Although they are convenient, not all clouds meet the same standards of security.[25] Due to a lack of security standards, 43% of security breaches in the United States are related to health data. These attacks originate both internally and externally.[25] Every human touchpoint is a potential security risk. To ensure patient privacy, Health Insurance Portability and Accountability Act (HIPAA) was established in 1996.[25] Despite revisions and updates, HIPAA cannot fully address the rapid advances in technology. Any database or software can be used if it is HIPAA compliant despite security risks.

Blockchain could revolutionize security through decentralization of data across a shared platform, all while maintaining security[14] through audit trails of access authorization.[26] On a blockchain, records tampering would be immediately evident through mismatch between ledgers. It is believed that blockchain could eliminate ransomware and protect patient privacy[2] beyond the current HIPAA requirements.

Permissioned blockchains would allow patients to control access to their records using digital keys (or asymmetric key cryptography that uses public and private key pairs). Everyone participating in the blockchain would have a private and a public key that would be cryptographically connected.[4] The public key would be available to view by everyone on the chain, but access to any identifying data would be limited to those utilizing the corresponding private key (the patient or authorized provider).[4,11,14] Patients could set up special permission scenarios using smart contracts.[11]

Security would be strengthened through the transparency of the public ledger as well. Without a centralized database, it is difficult to falsify or alter records. This would hold patients and providers accountable and discourage altering records.[27] Because a blockchain can update in near real time, the data would always be current. This could prevent human error from fewer interactions with data.[26,28]

Building off hashes makes the chain more secure, thus making blockchains resistant to attacks.[28] To be successful, hackers would have to attack

the target and every subsequent block built off it simultaneously to avoid any detection.[2] This is cost prohibitive as well as a major challenge for hackers.

COST SAVINGS

Just as the mechanization improved efficiency and reduced cost of production during the industrial revolution, similar cost savings could be available within healthcare. If the healthcare industry took full advantage of all available technological capabilities, trillions of dollars of efficiency could be possible through improving access to data and patients. McKinsey & Company conducted a study, which concluded that more than $300 billion could be saved per year by using already available siloed data.[29] By leveraging current technology data could be readily accessible, and the doctor–patient connection could be greatly improved through reliable patient histories and improved communication.[28,30]

Because blockchains do not depend on third-party goods and services, the savings are immediate and require very little effort on the part of the provider.[27] Doctors would no longer have to pay for hard copy record storage or file rooms and would require fewer administrative staff. The cost of cloud computing, for example, is heavily reliant on the fees associated with the services. It is also the cost of performance issues, process bottlenecks around data transfers, and the risk of the having to revert to in-house data storage due to the volatility of a third-party business model.[22] This uncertainty could impede productivity within a hospital or clinic. Blockchain technology would allow healthcare providers to focus on their patients and worry less about availability and organization of data.[29] Ideally, a combination of cloud-based storage and blockchain technology would allow for stable and fully digitized records management while requiring less human administration.

A reduction in staff would not be possible without automation. A revolutionary aspect of blockchain technology is the availability of automation through smart contracts. Blockchains are versatile and can be combined with other technologies to allow for previously human-intensive activities like claims adjudication to be done automatically by using smart contracts.[30] Smart contracts allow a programmable blockchain to blossom. Smart contracts are programmed to always function in the same manner and therefore can be trusted to perform exactly as specified.[29] This results in fewer transactions being blocked due to disagreements between systems.[31] Automation allows for fewer administrative staff, thus saving significant amounts of money. Practices in the United States spent $70 billion on paperwork alone in 2012, while hospitals spent $74 billion.[22] Smart contracts translate to less human interaction, which reduces cost of doing business and limits the possibility of data being lost, sold, or stolen.

DECREASE FRAUD

While rapid claims processing is important for revenue, to have an accurate claim the information must accurate. In 2016 alone, Medicare lost $30 million to fraud.[22] Approximately 50% of fraud is from superfluous billing or charging for services never rendered.[22] Currently, it is difficult to know where and when an order originated due to differing data storage practices between EHRs.[32] The basic functionality of blockchain technology makes fraud very difficult. To defraud is a covert operation. Blockchain would alleviate the burden of proving fraud through transparent, immutable records. Because each transaction is a record of who did what and on what date.[32]

The transparency of blockchain could also help address drug-seeking behaviors by patients through a record of access and transactions.[22]

Without the ability to view treatment information and histories, healthcare providers have little defense against "doctor shopping" by patients seeking prescriptions for controlled substances.[22,33]

The proof of concept blockchain Nuco (a founding member and director of the Enterprise Ethereum Alliance) is working to combat prescription drug abuse through a system of accountability.[20] Upon prescribing an opiate, a randomized machine-readable code is issued to that prescription to function as a specific identifier, which is associated with an information block that includes data such as the drug name, quantity, and the fully anonymized identity of the patient as well as when it was prescribed.[20] This allows for accountability without stigma. Blockchains would make a lasting impact on the opiate crisis through responsible prescribing and accountability. This would help patients who need pain relief without the fear of contributing to abuse. The use of a blockchain could clearly illustrate when, where, and how many opiates were prescribed to the patient or by a physician. Accountability could discourage doctor shopping as well as overprescribing.

BLOCKCHAIN ADOPTION CHALLENGES

Challenges facing blockchain include interoperability, scalability, vulnerability, security of patient data, data ownership, and information blocking.

Interoperability

Questions persist regarding interoperability. For example, will providers be on the same blockchain? Will it be public or private? Will each patient have their own personalized private blockchain? However, multiple models of digital ledgers create a new interoperability issue. Technologies are burgeoning; allowing communication cross-chain and off-chain open communication is still a work in progress.[34] Even with blockchain, the data structure issue persists between private and public chains.[21] Heterogeneous structures pose challenges for effective communication and data analysis.[21] For any model, data would be cryptographically secure, irrevocable, and easily exchanged.[22]

Currently, the capacity for storage within a blockchain is limited. The technology is not advanced enough to accommodate large files, so storing multitudes of complete medical records is not possible.[34] Private blockchains could address privacy and security issues, but they bring new risks of vendor lock-in and not utilizing the same open standards for data exchange.[17] Without an agreed upon coding standard, the same issues that currently plague interoperability would transfer to the blockchain.

Scalability

As previously mentioned, blockchain would have to function as an index due to issues with scalability. "The factors influencing scalability are bit rate, the frequency of monitoring and transmission, and the amount of information transmitted per patient."[35] If healthcare records utilized the Bitcoin blockchain, every node on the chain would have a copy of the ledger, which would not only cause issues with latency and block size limits, but also bring questions of security to light.[17,36] In addition, throughput is limited in the number of transactions and computing power of a node to increase efficiency of transaction processing.[22] The existing infrastructure of blockchain focuses on security and integrity over scalability and plasticity so addressing lag due to volumes of transactions would be difficult.[29] Also, each node would have a copy of every patient record stored on the chain across the country—a concept that is neither currently feasible nor secure.

What is possible is to use permissioned or private blockchains that utilize scalable data repositories called data lakes to store records off chain.[17] Data lakes would allow more functionality such as interactive queries, text mining, and machine learning.[2] Data lakes would be maintained and located at point of origin (provider nodes), assuming providers already function on secure networks.[24] All records would be cryptographically signed to guarantee authenticity and file integrity.[2]

Vulnerability

Blockchains are still vulnerable to malfunction and human errors.[22] The decentralized autonomous organization (DAO) attack proved that blockchain is not unassailable. DAO is a system that exists on the Ethereum blockchain whose processes can be modified if certain criteria encoded in a smart contract are met.[37] The DAO was a crowd-funded initiative that allowed investors to vote on and potentially invest in project proposals by startups on the chain.[38] Quickly, $168 million in ether was amassed from potential investors.[37,38] Hackers were able to siphon off $50 million in ether simply by exploiting a flaw in the code of the smart contract.[37] Codes originate from humans and therefore are subject to human error and exploitation by proxy.

Even beyond the blockchain itself, vulnerabilities exist. In any situation, a reliance on the security of the originating EHR or personal computer would be unavoidable.[9,24] Blockchains are not antiviral in nature, thus systems are still open to ransomware attacks.[34] Up to 43% of system attacks were carried out from within the system, while 27% was due to external attacks such as hacking and ransomware.[22]

The risk for security breaches only grows as the chain ages. Without proper maintenance of code used to implement the chain, the chain becomes more vulnerable to attacks.[28] Furthermore, the encryption used could be exploited and leave any information open for decryption.[18,39] To combat this, a third party would have to audit the system; this defeats the purpose of the public blockchain. It would be more accurate to say that blockchains are resistant to tampering rather than completely secure or tamper proof.

Security of patient data

The primary concern with sensitive data is responsible handling and security. On a public blockchain records would be disseminated across every node without cryptographic signatures; data would be available for anyone to access. Due to the immutable nature of the blockchain, all data attached to the blockchain would remain open to indefinite public viewing.[28] Thus, the lack of security due to uncontrolled access not only makes the Bitcoin blockchain inappropriate,[17] but it would also be noncompliant with HIPAA standards for handling protected health information (PHI).

Any public blockchain that stored patient records would have to insure complete privacy. This could be accomplished by using pseudonyms, but this does not guarantee complete anonymity. Connections could still be drawn about the identity of the patient from the metadata of another node.[9,24] This is a direct violation of HIPAA, which expressly states that all PHI must be expunged from all medical data before sharing.[30]

Data ownership

HIPAA states that patients own their data and should have unfettered access to them.[29] Compliance aside, many systems feel they own the data because it originated with them,[40] and any patient ownership is negligible.[19] In traditional models, patients are not able to revoke access to

their records. Thus, data are siloed and hoarded for permanent possession.[18] A patient may see many different doctors over their lifetime. If every provider feared to share data due to losing competitive advantage or decreasing patient retention,[21] the resulting data fragmentation could leave the data vulnerable to attack.[18] HIPAA is counterintuitive to interoperability. It states that as little information as possible should be shared to protect patient data while still conveying the methods of care.[41] This sum of the refusal or reluctance to share data is known as information blocking.

Information blocking

Information blocking has been defined by law to be "any practice that ... is likely to interfere with, prevent or materially discourage access, exchange or use of electronic health information." Proving intent to keep information (information blocking) is difficult to prove. Being greedy with data is not limited to systems; 49% of providers surveyed stated that EHRs routinely block information through intentionally limiting interoperability, charging high fees for exchanges, and making third party access difficult or impossible.[41] Blockchain could combat information blocking by making patients the stewards of their own records,[30] but de-soling data may prove difficult.

In 2016, the Cures Act became law, which directed the ONC to create a framework of rules and enforcement agencies to prevent information blocking.[27] Included in the legislation was the ability to wager stiff penalties for instances of information blocking, up to 1 million per violation.[27]

In a time where data are capital, EHR vendors are routinely opaque in their practices. Huge competition exists within the EHR market. EHR vendors gain more revenue through guarding information and charging systems to modify it,[30] so much so that the vendors are oftentimes more likely to engage in blocking.[41] Without a log to understand when and how this happens, it is difficult to prove the information was knowingly blocked. Blockchain could change that, but would require cooperation from vendors.

DISCUSSION AND CONCLUSIONS

While many functions of healthcare can be streamlined using technology, fragmentation and data transference have not been resolved in the United States. The combination of resistance, lack of mandates, and outdated HIPAA guidelines mean there is very little movement toward interoperability. While blockchain technology could revolutionize or at least improve interoperability, the technology is still not fully developed.

Issues of scalability and privacy mean that developing platforms or useful applications are difficult. It is evident that within 10 years the blockchain technology will evolve to meet the needs of consumers. Just as the Internet evolved rapidly and changed communication, blockchain can grow to meet the needs of healthcare.

The versatility and simplicity in the concept of blockchain make it a very attractive answer to conundrums faced by businesses today. The promise of a transparent ledger seems so simple in concept, but in application it becomes difficult. Without government intervention to force interoperability it will take consumer demand to place pressure on the healthcare establishment to improve information sharing.

Blockchain technology in its current form will not be able to live up to its potential for record sharing. It will take time, focus, and more use cases to bring blockchain to the forefront of healthcare. Blockchain might be used successfully in healthcare globally before

it is able to be used on a large scale in the United States. The very ideas of governance and profitability that have driven the United States to be a superpower may be the biggest hindrance to the adoption and interoperability. Without HIPAA reform and/or improved data security surrounding privacy, governance will continue to stifle potential adoption. Similarly, without the cooperation of vendors who may risk the potential loss of profits, records may never make it to the blockchain to be shared.

Healthcare is a business, thus it strives to maintain a profit. Blockchain could help improve profits and improve the quality of care for patients through decreasing fraud and increasing savings for doctors.

As technology advances, more solutions to current problems will arise with blockchain. Currently, the three models of blockchain discussed in this article have very distinct advantages and disadvantages depending upon the situation. For example, the Bitcoin chain works well when privacy is not a concern. The Ethereum chain would be ideal for situations where automation is required. It is still not well suited for data storage and throughput may be an issue for large volumes of claims though. Hyperledger's private design is more suited for PHI, but current limitations such as data silos and legal constraints make it difficult to implement.

The future of blockchain in healthcare is undeniably bright. As demand drives innovation, the current limitations can be overcome. To resolve current issues facing healthcare, it will take reconciliation between technologies such as blockchain, cloud storage, and emerging technologies to deliver higher quality patient-centered care. Currently, advances are being made in open sourced distributed ledgers that utilize different consensus protocols to verify transactions and improve verification time. These solutions allow for greater throughput and are more scalable; however, a more detailed explanation is beyond the scope of this article. The blockchain and distributed ledger transformation of healthcare are close, but nothing is achievable overnight and not without the effort of the healthcare community as a whole.

Financial Statement: The authors received no financial support to conduct this study.

Contributors: Gracie Carter was the principal author and conducted the research. Denise White was the contributing author and did the research. Anusha Nalla conducted the research. Hossain Shahriar performed editorial and advisory roles for this study. Sweta Sneha played an advisory role in the conduct of this research.

Conflicts of Interest: The authors declare no competing interests with respect to research, authorship, and/or publication of this article.

REFERENCES

1. Kim D, Kagel JH, Tayal N, Bose-Brill S, Lai A. The effects of doctor-patient portal use on health care utilization rates and cost savings. *SSRN Electronic J*. [Internet]. (39) 2017. doi:10.2139/ssrn.2775261
2. Linn LA, Koo MB. "Blockchain for health data and its potential use in health it and health care related research." *Proc ONC/ NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, MD, USA: ONC/NIST; 2016:1–10.
3. NHE -Fact-Sheet [Internet]. CMS.gov Centers for Medicare & Medicaid Services. 2019. Available from: https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NHE-Fact-Sheet.html (accessed March 10, 2018).
4. Blumenthal D, Tavenner M. The "meaningful use" regulation for electronic health records. *N Engl J Med*. 2010;363(6):501–4.

5. Lapsia V, Lamb K, Yasnoff WA. Where should electronic records for patients be stored?. *Int J Med Informat*. 2012;81(12):821–7.
6. Bosworth HB, Zullig LL, Mendys P, et al. Health information technology: Meaningful use and next steps to improving electronic facilitation of medication adherence. *JMIR Med Informat*. 2016;4(1):e9. Doi:10.2196/medinform.4326
7. Koppel R, Lehmann CU. Implications of an emerging EHR monoculture for hospitals and healthcare systems. *JAMIA*. 2014;22(2):465–71.
8. 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 & Big Data (OBD)* [Internet] 2016 Aug 22 (pp. 25–30). IEEE.
9. Studeny J, Coustasse A. Personal health records: Is rapid adoption hindering interoperability? 2019 Winter. *Perspect Health Inf Manag*. 2019;16(Winter):1a.
10. Ahuja SP, Mani S, Zambrano J. A survey of the state of cloud computing in healthcare. *Netw Commun Technol*. 2012;Dec 1;1(2):12.
11. Kuo AMH. Opportunities and challenges of cloud computing to improve health care services. *JMIR.* 2011;13(3):e67.
12. Zhang R, Liu L. Security models and requirements for healthcare application clouds. In *3rd International Conference on Cloud Computing (CLOUD)*.) *[Internet]*. IEEE; 2010. Available from: http://dx.doi.org/10.1109/cloud.2010.62. pp. 268–275.
13. Leventhal R, Top Ten Tech Trends 2017: Blockchain's promise has healthcare innovators eager. 2017. Available from: https://www.healthcare-informatics.com/article/interoperability/blockchain-s-promise-has-healthcare-innovators-eagerPage.
14. D'arcy GG. Why blockchain offers a fresh approach to interoperability. *Health Data Manag*. 2017. Available from: https://www.healthdatamanagement.com/opinion/why-blockchain-offers-a-fresh-approach-to-interoperability, (accessed March 10, 2018).
15. Sandner P. Comparison of Ethereum, Hyperledger Fabric and Corda. Medium 2017. https://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6 (accessed June 11, 2018).
16. Zhang P, Walker MA, White J, Schmidt DC, Lenz G. Metrics for assessing blockchain-based healthcare decentralized apps. In *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*. 2017 Oct 12. pp. 1–4. IEEE. https://www.dre.vanderbilt.edu/~schmidt/PDF/IEEE-Healthcom-2017.pdf. (accessed 6/11/19).
17. Ekblaw AC. MedRec: Blockchain for medical data access, permission management and trend analysis. Doctoral dissertation, Massachusetts Institute of Technology. 2017. https://dspace.mit.edu/handle/1721.1/109658 (accessed 6/11/19).
18. Winfield, L. A look at the Trump administration's approach to HIT. Healthcare Financial Management Association. https://www.hfma.org/Content.aspx?id=59347 (accessed June 11, 2019).
19. Ahier B. Three rising technologies that will impact healthcare in 2018. Available from: Healthdatamanagement.com. 2018 Jan 5;1.
20. Rabah K. Challenges and opportunities for blockchain powered healthcare systems: A review. *Mara Res J Med Health Sci*. 2017; Oct 16;1(1):45–52.
21. Engelhardt MA. Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. *Tech Innovat Manag Rev.* 2017;7(10): 22–34.
22. Arndt RZ. The long and winding road to patient data, interoperablility. *Mod Healthc.* 2017 May;47(18):16–18.
23. Sneha S, Varshney U. Enabling ubiquitous patient monitoring: Model, decision protocols, opportunities and challenges. *Decis Support Syst.* 2009. Feb 1;46(3):606–19.
24. Peterson K, Deeduvanu R, Kanjamala P, Boles K. A blockchain-based approach to

health information exchange networks. In *Proc. NIST Workshop Blockchain Healthcare*, 2016;1:1–10. https://www.sciencedirect.com/science/article/pii/S0167923608002030 (accessed 6/11/19).
25. Mettler M. Blockchain technology in healthcare: The revolution starts here. [Internet] In 2016 *IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)* 2016 Sep 14. pp. 1–3. IEEE.
26. Ichikawa D, Kashiyama M, Ueno T. Tamper-resistant mobile health using blockchain technology. *JMIR MHealth UHealth*. 2017;5(7):e111.
27. Nye J. How blockchain could help boost healthcare security. Available from: Healthdatamanagement.com [Internet]. 2017 Sep 2:1, (accessed March 1, 2018).
28. Dhanireddy S, Walker J, Reisch L, Oster N, Delbanco T, Elmore JG. The urban underserved: Attitudes towards gaining full access to electronic medical records. *Health Expectations*. 2014 Oct;17(5): 724–32.
29. Lemieux VL. Trusting records: Is Blockchain technology the answer? *Record Manag J.* 2016 Jul 18;26(2):110–39.
30. Salahuddin MA, Al-Fuqaha A, Guizani M, Shuaib K, Sallabi F. Softwarization of Internet of things infrastructure for secure and smart healthcare. [internet] arXiv preprint arXiv:1805.11011. 2018 May 28.
31. Halamka JD, Ekblaw A. The potential for blockchain to transform electronic health records. *Harv Bus Rev.* 2017 Mar 3;3. (about 3 pages).
32. Haughwout J. Tracking medicine by transparent blockchain. *Pharmaceutical Process*. 33(1), 24–26.2018.
33. Slabodkin G. Blockchain remains a work in progress for use in healthcare. *Health Data Manage*. 2017;25(3):37–39.
34. Ozkaynak M, Flatley Brennan P, Hanauer DA, et al. Patient-centered care requires a patient-oriented workflow model. *JAMIA*. 2013 Mar 28;20(e1):e14–16.
35. Varshney R., The non financial side of Blockchain. Mumbai: Express Computer; 2016.
36. Zhang P, White J, Schmidt DC, Lenz G. Applying software patterns to address interoperability in blockchain-based healthcare apps. [internet] arXiv preprint arXiv:1706.03700.2017 June 5.
37. Adler-milstein J, Pfeifer E. Information blocking: Is it occurring and what policy strategies can address it? *The Milbank Quarterly*. 2017 Mar;95(1):117–35.
38. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of things. *IEEE Access.* 2016;4:2292–303.
39. Mehar MI, Shier CL, Giambattista A, et al. Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. *JCIT*. 2019 Jan 1;21(1):19–32.
40. Ivan D. Moving toward a blockchain-based method for the secure storage of patient records. InONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, MD, United States: ONC/NIST; 2016.
41. Chang JL. The dark cloud of convenience: How the HIPAA omnibus rules fail to protect electronic personal health information. *Loy. LA Ent. L. Rev.* 2013;34:119.