

Influential Article Review - Approaches for Integrated Medical Infrastructure Utilizing Blockchain Technology

Pierre Marriott

Rikki Parkes

Nyle Rose

This paper examines system innovation. We present insights from a highly influential paper. Here are the highlights from this paper: With a growing trend in medicine towards individualized, patient-centric care, traditional health information technology limits progress. With high administrative costs and the lack of universal data access, contemporary electronic medical records serve more the institution rather than the patient. Blockchain technology, as presently described, was initially developed for use in financial markets, serving as a decentralized, distributed ledger of transactions. However, certain inherent characteristics of this technology suit it for use in the healthcare sector. Potential applications of the blockchain in medicine include interoperable health data access, data storage and security, value-based payment mechanisms, medical supply chain efficiency, amongst others. While the technology remains in nascent stages, it is essential that members of the healthcare community understand the fundamental concepts behind blockchain and recognize its potential impact on the future of medical care. For our overseas readers, we then present the insights from this paper in Spanish, French, Portuguese, and German.

Keywords: blockchain, electronic medical records, data security, interoperability

SUMMARY

- A summary of the benefits and drawbacks of the use of blockchain in healthcare can be visualized in Table 1.
- Currently, there exists a significant challenge distributing medical records across health care platforms, for example, between a nursing home and an acute care center or even between two independent hospitals. This leads to inefficiencies in health data collection and failures to communicate essential health information such as medications and allergies. However, by using novel technologies, a health system can assimilate an individual's medical record into a block, which can then be cryptographically stored in nodes across a distributed blockchain, accessed remotely by permitted providers, and updated with new relevant medical information. This would obviate the need for patients to bring paper or electronic records to a new health care environment; they would simply allow the provider to access to their medical data on the blockchain.

- Several platforms are currently being developed to address optimal interoperability of electronic health records.
- Several characteristics of a blockchain infrastructure allow for a more secure data maintenance and transfer system, compared to current standards. First, the distributed ledger system fundamentally records an immutable history of transactions. When a patient's data is accessed, the event is incorporated into the permanent chain, which is then simultaneously updated on all nodes across the network.
- The ability to encode smart contracts within various blockchain infrastructures permits a more efficient value-based healthcare payment model. An insurance payer, for example, may encode reimbursement for a physician to be fulfilled only when certain conditions are met on the blockchain. In this instance, the common mistrust between physician and payer is eliminated.
- Maintaining an immutable identification source using blockchain technology would have significant impact for both patients and practitioners. Similar to traditional identification verification, individuals will be able to have their identities confirmed using a combination of personal, government, and financial records.
- With big data, artificial intelligence, and machine learning emerging as revolutionary scientific instruments, a healthcare blockchain infrastructure could permit more effective medical research. With a large, standardized, de-identified data registry, research institutions could perform more significant clinical trials and prospective analyses. Amassing and analyzing information-heavy data sets, such as tumor genomics, would allow for a more personalized medicine.
- As opposed to existing EMR systems in which the medical data are controlled by the clinician, securing medical data on the blockchain allows the patient to become the primary intermediary in distributing his or her medical information.
- The current global medical supply chain, consisting of pharmaceuticals, medical devices, and hospital goods, is fractionated and inefficient. Substandard, expired, or counterfeited products directly threaten patient care. A distributed ledger technology permits several advantages over the current supply chain delivery.

HIGHLY INFLUENTIAL ARTICLE

We used the following article as a basis of our evaluation:

Schot, J., & Steinmueller, W. E. (2018). Three frames for innovation policy: R&D, systems of innovation and transformative change. *Research Policy*, 47(9), 1554-1567.

This is the link to the publisher's website:

<https://www.sciencedirect.com/science/article/pii/S0048733318301987>

INTRODUCTION

In January 2015, President Barack Obama enacted the Precision Medicine Initiative, which aimed “to enable a new era of medicine through research, technology, and policies that empower patients, researchers, and providers to work together toward development of individualized care” [16]. With an intensified focus on treating individual patients and not their disease processes, comes the fundamental need for accurate clinical data that can be widely distributed to healthcare providers in an efficient, secure manner. Although the mandatory use of EHRs was established via the U.S. Centers for Medicare and Medicaid Services (CMS) Meaningful Use criteria in 2009 [1], the broad array of economically competing EHRs used in different hospital systems significantly limits interoperability and prevents fluid exchange of health information between institutions. As a result, a patient's individual medical record can be significantly

fragmented across the health system, with important documents such as medical history, medication list, and advance directives potentially unavailable in emergency situations.

In the modern era of information technology, an increasing amount of data is being transmitted and stored on cloud-based networks. As defined by the U.S. National Institute of Standards and Technology (NIST) [9], cloud computing is “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources.” Cloud computing has proven ideal for such Internet services as information sharing, file backup, and big data analytics, where cost-effectiveness and optimal resource utilization are essential. Thus, given the vast quantities of medical information generated daily, there has been a recent push towards cloud-based storage and distribution of health care data. However, a centralized, shared data repository presents the risk of cybersecurity breach and directly challenges a patient’s individual right to privacy.

Herein lies the complexity of designing a functional health information system that still maintains the core principles of a medical record, mainly comprehensiveness, accessibility, interoperability, confidentiality, accountability, and flexibility [7]. In 2014, the U.S. Office of the National Coordinator for Health Information Technology (ONC) presented its 10-year vision to achieve a universal Health IT infrastructure [14], stating that “this goal will only be possible with a strong, flexible health IT ecosystem that can appropriately support transparency and decision-making, reduce redundancy, inform payment reform, and help to transform care into a model that enhances access and truly addresses health beyond the confines of the health care system.” The foundation of a new healthcare information technology system must be rooted in platform interoperability, such that data storage and access are standardized, patient safety and confidentiality is prioritized, and a dedication to patient-centric care is maintained.

BLOCKCHAIN TECHNOLOGY

Recently, there has been intense focus on the development of blockchain-based technologies around the world. At its most elemental level, a “blockchain” is a decentralized, distributed ledger of digital transactions that allows a trustless exchange of money or data. In existing payment models, such as credit card, money order, or electronic (ex. PayPal) transactions, a third-party intermediary exists to facilitate exchange. Within a traditional transaction, the presence of a centralized institution, with inherent financial incentives, introduces the possibility of bias, dishonesty, and, ultimately, fraud. Furthermore, even with current financial technologies, the inefficient processes of transactional verification can take days before money is withdrawn from one account and deposited in another. Considering these drawbacks to contemporary financial instruments, blockchain technology has developed over time to address the fundamental problems of transactional trust, speed, and integrity.

Initially described in 2009 by the anonymous individual or group known as Satoshi Nakamoto, the Bitcoin blockchain was developed as a peer-to-peer electronic cash system [10]. The blockchain functions by sequentially adding encrypted blocks of transactions to a chain, and simultaneously distributing the updated chain to specified nodes across a network. Thus, since the updated blockchain is reliably distributed, the transactions within the individual blocks are immutable, and the integrity of the blockchain can be verified. Public identification keys are used between individuals in a transaction, and the payer cryptographically signs transactions using a hidden private key, known only to the payer. Miners within a blockchain are nodes that construct blocks of transactions to be added to the chain and are incentivized to work by collecting transaction fees. Thus, it is through the miners that a consensus blockchain is built and distributed to the rest of the network.

Since the origin of Bitcoin, other competing cryptocurrencies have emerged, each with a unique distributed ledger of transactions, but based on a variable blockchain code structure. Some blockchain technologies, such as Ethereum, allow space in blocks to include “smart contracts,” or lines of code that define self-executing and/or self-enforcing clauses, running only if certain conditions are met. Most platforms have user-owned tokens that can be used to pay transaction costs, encode smart contracts, or transfer data between individuals on the blockchain. As these technologies have developed significant value in recent years, new platforms can use an “Initial Coin Offering (ICO)” to obtain early funding. These coins

can be publicly traded on cryptocurrency exchanges, an enigmatic financial sector which had a market capitalization of over \$800 billion in January 2018 [8]. Since peaking in value in January 2018, however, cryptocurrency exchanges have lost approximately 80% of their value, reflecting overvaluation in the face of slow adoption by various economic industries [11].

Regardless, the fundamental principle of a blockchain, mainly the anonymous, distributed ledger of transactions, remains relevant and still lends itself to certain technologic applications, such as distributed cloud storage, encrypted digital identification, and decentralized payment strategies. Here, the parallels between blockchain technology and the core needs of the modern health care infrastructure are apparent [4, 6, 13]. In the following section, we review several potential solutions that blockchain technologies address in the current health IT landscape.

LIMITATIONS OF THE BLOCKCHAIN IN HEALTHCARE

The foundational benefit of a blockchain infrastructure is its shared, non-modifiable record of transactions. However, the fact that data is shared amongst all participants in a network may seem to undermine the necessary anonymity of protected health information (PHI). This can be addressed by incorporating only de-identified and encrypted data into the blockchain. Whereas information in the blockchain itself is public, PHI stored in data repositories off the blockchain would be heavily protected and HIPPA compliant. Again, accessing this data would only be permissible by the patient, using smart contracts and an anonymous private key to limit access to only specified clinicians. Managing this private key may prove difficult for the individual patient, especially for the elderly or disabled population, but precise biometric linking to one's key may obviate a physical record. Furthermore, maintaining a confidential private key is no different than protecting a social security number or institutional medical record number for medical data access. The true strength of blockchain technology lies in its ability to confirm with complete certainty that a transaction or an event has taken place, without compromising the specific information of the event.

Distributed data sharing requires a network of nodes to build and maintain the blockchain. This poses two problems. First, creating such a healthcare network requires significant buy-in from the medical community. Existing medical systems preserve the status quo, and a novel healthcare infrastructure may prove too expensive or difficult for widespread implementation. Second, maintaining a blockchain network requires significant computing power, which can lead to greater cost of hardware and energy consumption by a hospital system. In both cases, incentivizing participants in the healthcare blockchain may lead to its greater utilization. Blockchain-based applications may distribute tokens to participants in the network, which can be exchanged for services such as increased data storage, faster data transfer, or access to a data repository. Tokens can also be traded for Bitcoin or U.S. dollars on a cryptocurrency exchange, allowing the option for direct financial compensation.

Lastly, as it stands now, private medical data is highly protected by both the individual and his or her medical institution. By claiming ownership over a large amount of health records, hospitals and practices monetize data sharing with researchers and industry partners (ex. clinical trials and public health studies). The movement towards decentralized data storage and distribution on a blockchain may encounter significant pushback by institutions that value medical data ownership. Fundamentally shifting the ownership of personal health records to the patient will require a philosophical paradigm shift in both health policy and law.

CONCLUSIONS

In the coming years, there will be revolutionary advances in the global health IT infrastructure. Emerging technologies will serve to address issues with the current system, including the lack of interoperability of electronic health record (EHR) software, the inefficient and insecure transfer of protected health information (PHI), an ineffective payment system for value-based care, and the evolving need for patient-centered care. Creating and implementing a blockchain-based healthcare network can address these

problems in a revolutionary way. As novel technologies are developed, it is up to clinicians to maintain an accepting, yet inquisitive attitude, a willingness to implement new ideas, and a philosophy of feedback rather than absolute dismissal.

REFERENCES

- Bhowmick, S., Young, J.A., Clark, P.W., & Bhowmick, N. (2017). Marketing Students' Mathematics Performance: The Mediating Role of Math Anxiety on Math Self-Concept and Math Self-Efficacy. *Journal of Higher Education Theory and Practice*, 17(9). <https://doi.org/10.33423/jhetp.v17i9.1426>
- (CMS) C for M and MS. Electronic Health Records (EHR) Incentive Programs (2017). Retrieved July 16, 2017, from <https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms>
- Cunningham J., & Ainsworth J. (2017). Enabling Patient Control of Personal Electronic Health Records Through Distributed Ledger Technology. *Stud Health Technol Inform.*, 245, 45–48. <https://doi.org/10.3233/978-1-61499-830-3-45>
- Ekblaw, A., Azaria, A., Halamka, J.D., & Lippman, A.A (2016). Case Study for Blockchain in Healthcare: MedRec prototype for electronic health records and medical research data. Retrieved July 29, 2017, https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf
- Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *J Med Syst.*, 42(8), 136. <https://doi.org/10.1007/s10916-018-0993-7>
- Health Level Seven International. FHIR v3.0.1. (2017). Retrieved July 30, 2017, from <https://www.hl7.org/fhir/overview.html>
- Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., & Liu, S. (2018). Blockchain-Based Data Preservation System for Medical Data. *J Med Syst.*, 42(8), 141. <https://doi.org/10.1007/s10916-018-0997-3>
- Mandl, K.D., Szolovits, P., & Kohane, I.S. (2001). Public standards and patients' control: How to keep electronic medical records accessible but private. *BMJ.*, 322(7281), 283–7. <https://doi.org/10.1136/bmj.322.7281.283>
- Marshall, A. (2018, January 7). *Combined Crypto Market Capitalization Races Past \$800 Bln*. CoinTelegraph. Retrieved June 6, 2017, from <https://cointelegraph.com/news/combined-crypto-market-capitalization-races-past-800-bln>
- Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. Retrieved July 16, 2017, from <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>
- Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System; 2009. Retrieved July 16, 2017, from www.bitcoin.org
- Patterson, M. (2018). *Crypto's 80% Plunge Is Now Worse Than the Dot-Com Crash*. Bloomberg. Retrieved October 23, 2018 from <https://www.bloomberg.com/news/articles/2018-09-12/crypto-crash-just-surpassed-dot-com-levelsas-losses-reach-80>
- Peterson, K., Deeduvanu, R., Kanjamala, P., Boles, K., & Clinic, M.A. (2017). *Blockchain-Based Approach to Health Information Exchange Networks*. Retrieved July 30, 2017, from <https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf>
- Radanović, I., & Likić, R. (2018). Opportunities for Use of Blockchain Technology in Medicine. *Appl Health Econ Health Policy*, 16(5), 583–590. <https://doi.org/10.1007/s40258-018-0412-8>
- The Office of the National Coordinator for Health IT. (2014). *Connecting Health and Care for the Nation: A Ten Year Vision to Achieve Interoperable Health IT Infrastructure*. Retrieved July 16, 2017, from <https://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf>
- Wang, H., & Song, Y. (2018). Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. *J Med Syst.*, 42(8), 152. <https://doi.org/10.1007/s10916-018-0994-6>

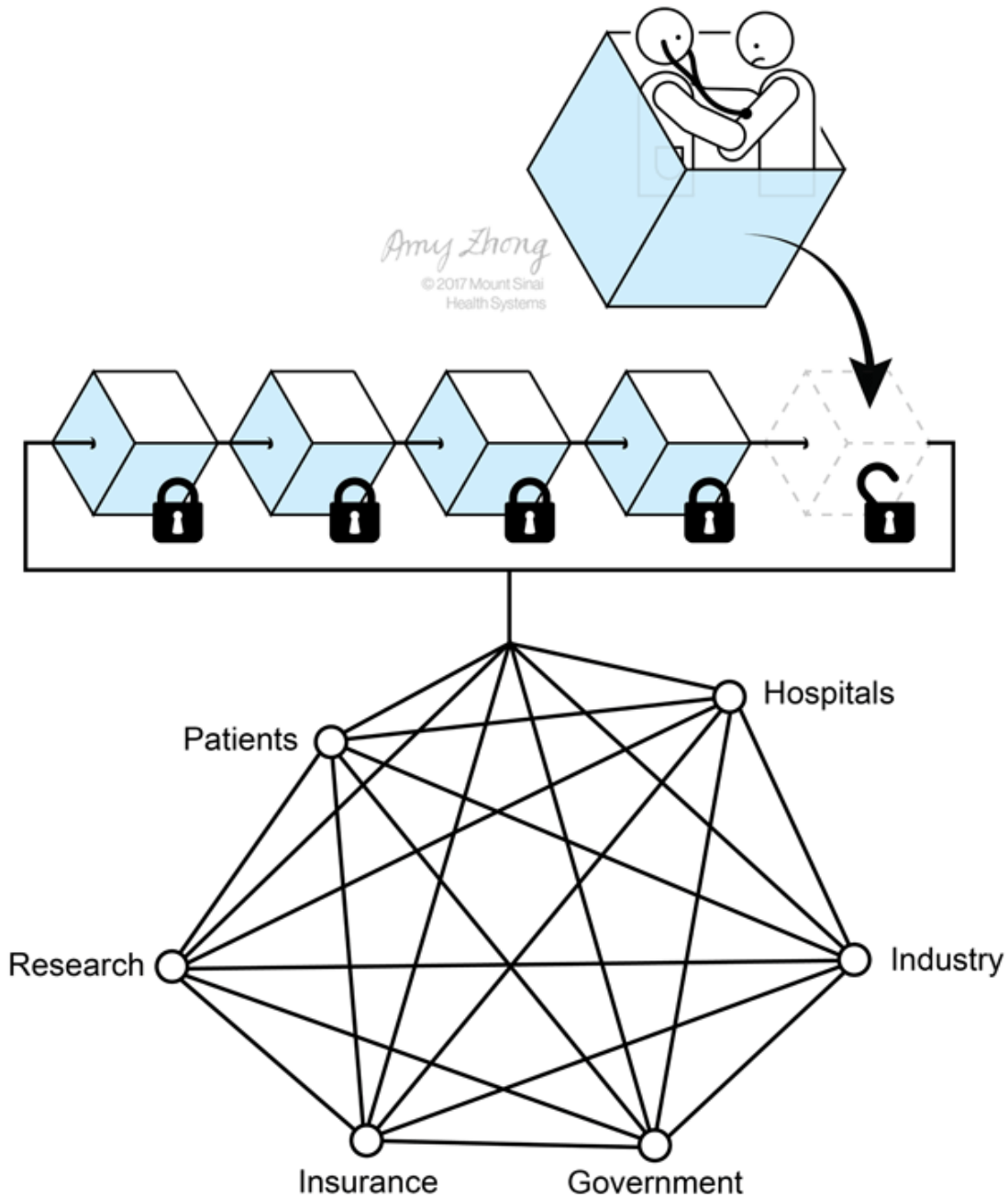
White House O of the PS. Precision Medicine Initiative. The White House Archives. (2015). Retrieved July 16, 2017, from [https:// obamawhitehouse.archives.gov/precision-medicine](https://obamawhitehouse.archives.gov/precision-medicine)

APPENDIX

**TABLE 1
FUNDAMENTAL BENEFITS AND DRAWBACKS OF BLOCKCHAIN TECHNOLOGY OVER
CONTEMPORARY FINANCIAL SYSTEMS**

BENEFITS	
Decentralization	Parties transact without a third-party intermediary, reducing financial bias and fraud
Trustlessness	Financial balances secured on the blockchain, payments made only when balance available
User-centricity	Individuals, rather than institutions, in control of personal financial data; identity verification
Transparency	All transaction data publicly available on the distributed ledger
Immutability	Distributed ledger contains precise history of all prior transactions and balances, making alterations impossible
Speed	Inefficient transaction verification process between financial institutions unnecessary; transactions processed 24/7
Simplicity	Single distributed ledger contains all current balance and transaction histories
Cost	Removing intermediaries saves on transaction fees
DRAWBACKS	
Technology	Blockchain software is still in its infancy, continually being developed and refined
Integration	Must initially be co-existent with current financial technologies, must be integrated overtime
Cost	Adoption of new technologies will incur initial greater costs to institutions
Regulation	Government institutions have yet to settle regulatory concerns over blockchain technology
Culture	Adoption of the technology will require significant buy-in from the global community
Energy	Maintaining the blockchain requires a network of nodes, and resulting substantial computing power
Privacy	Emerging cyber security concerns must be addressed before individuals will entrust data to a public blockchain

FIGURE 1
THEORETICAL SCHEMATIC OF BLOCKCHAIN TECHNOLOGY IN HEALTHCARE



During a healthcare interaction, medical data is recorded via an institutional EMR platform, and the resulting encrypted meta-data is incorporated into an individual “block”. This block is then presented to network participants for inclusion into the blockchain. When a block is incorporated into the blockchain, the entire chain is immediately distributed to all participants in the network, so that each has an identical copy of all data. The resulting blockchain is decentralized (no central authority has ownership), immutable (changing blockchain data at one node is immediately rejected by the consensus), and easily accessible from any network participant.

Source: Amy Zhong, Mount Sinai Health System.

TABLE 2
EMERGING BLOCKCHAIN SOLUTIONS IN HEALTHCARE INFORMATION TECHNOLOGY. PLATFORMS MAY BE THEORETICAL, IN DEVELOPMENT, OR IN CURRENT CLINICAL USE

Company	Solution	Description
Accenture (Dublin, Ireland)	Security	In partnership with Microsoft, developing blockchain-based identification system based on biometric data.
Blockchain Health (San Francisco, USA)	Data management	Provides HIPAA-compliant blockchain solutions for healthcare organizations; facilitates sharing of data with researchers..
Blockpharma (Paris, France)	Supply chain	Accesses pharmaceutical company records, allowing transaction auditing.
Bloq (Chicago, USA)	Data management	Offers services for institutions to create, test, and apply custom blockchain solutions.
Bowhead Health (Singapore)	Patient-centric care	Bowhead device accesses blockchain data to accurately dispense medication and track compliance.
Burst IQ (Denver, USA)	Data management	Manages large HIPAA-compliant data repository; monetizes data sharing.
Gem Health (Venice, CA, USA)	Data management	HIPAA-compliant blockchain platform; allows secure access to sharable data.
HealthCombix (Nashville, USA)	Patient-centric care, value-based payments	Blockchain platform prioritizing patient control of data; token-based payment system.
Health Wizz (Falls Church, VA, USA)	Patient-centric care	Platform allows patients to create a personal health portfolio; smart contracts allow payment for health data in cryptocurrency.
iSolve (Sandton, South Africa)	Supply chain	Organizes, schedules, and tracks delivery of medical devices and pharmaceuticals.
MedicalChain (London, England)	Interoperability	Secure storage of medical data on the blockchain; patients permit access to individual providers/institutions.
Patientory (Atlanta, USA)	Interoperability	Facilitates interoperability of existing electronic medical record systems (ie. Epic, Cerner, Allscripts).
PokitDok (San Mateo, CA, USA)	Value-based payments, supply chain	DokChain, a blockchain-based transaction ledger, focused on financial and supply chain management.
ScalaMed (Sydney, Australia)	Data management	Creating a decentralized platform for managing financial and data transactions.

TRANSLATED VERSION: SPANISH

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

VERSION TRADUCIDA: ESPAÑOL

A continuación se muestra una traducción aproximada de las ideas presentadas anteriormente. Esto se hizo para dar una comprensión general de las ideas presentadas en el documento. Por favor, disculpe cualquier error gramatical y no responsabilite a los autores originales de estos errores.

INTRODUCCIÓN

En enero de 2015, el presidente Barack Obama promulgó la Iniciativa de Medicina de Precisión, que tenía como objetivo "permitir una nueva era de la medicina a través de la investigación, la tecnología y las políticas que empoderan a los pacientes, investigadores y proveedores para trabajar juntos hacia el desarrollo de la atención individualizada" [16]. Con un enfoque intensificado en el tratamiento de pacientes individuales y no en sus procesos de enfermedad, surge la necesidad fundamental de datos clínicos precisos que puedan distribuirse ampliamente a los proveedores de atención médica de una manera eficiente y segura. Aunque el uso obligatorio de los EHR se estableció a través de los criterios de uso significativo de los Centros de Servicios de Medicare y Medicaid (CMS) de los Estados Unidos en 2009 [1], la amplia gama de EHR económicamente competidores utilizados en diferentes sistemas hospitalarios limita significativamente la interoperabilidad e impide el intercambio fluido de información de salud entre instituciones. Como resultado, el registro médico individual de un paciente puede fragmentarse significativamente en todo el sistema de salud, con documentos importantes como el historial médico, la lista de medicamentos y las directivas anticipadas potencialmente no disponibles en situaciones de emergencia.

En la era moderna de la tecnología de la información, una cantidad cada vez mayor de datos se transmite y almacena en redes basadas en la nube. Según la definición del Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) [9], la computación en la nube es "un modelo para permitir el acceso a la red ubicua, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables". La computación en la nube ha demostrado ser ideal para servicios de Internet como el intercambio de información, la copia de seguridad de archivos y el análisis de big data, donde la rentabilidad y la utilización óptima de los recursos son esenciales. Por lo tanto, dadas las grandes cantidades de información médica generada diariamente, ha habido un impulso reciente hacia el almacenamiento y la distribución de datos de atención médica basados en la nube. Sin embargo, un repositorio de datos centralizado y compartido presenta el riesgo de violación de la ciberseguridad y desafía directamente el derecho individual de un paciente a la privacidad.

Aquí radica la complejidad de diseñar un sistema de información de salud funcional que aún mantenga los principios básicos de un registro médico, principalmente la exhaustividad, la accesibilidad, la interoperabilidad, la confidencialidad, la responsabilidad y la flexibilidad [7]. En 2014, la Oficina del Coordinador Nacional de Tecnología de la Información en Salud (ONC) de los Estados Unidos presentó su visión de 10 años para lograr una infraestructura universal de TI de salud [14], afirmando que "este objetivo solo será posible con un ecosistema de TI de salud fuerte y flexible que pueda apoyar adecuadamente la transparencia y la toma de decisiones, reducir la redundancia, informar la reforma de pagos y ayudar a transformar la atención en un modelo que mejore el acceso y realmente aborde la salud más allá de los confines de la salud. sistema de cuidados". La base de un nuevo sistema de tecnología de la información de atención médica debe basarse en la interoperabilidad de la plataforma, de modo que el almacenamiento y el acceso a los datos se estandaricen, se priorice la seguridad y confidencialidad del paciente y se mantenga una dedicación a la atención centrada en el paciente.

TECNOLOGÍA BLOCKCHAIN

Recientemente, ha habido un intenso enfoque en el desarrollo de tecnologías basadas en blockchain en todo el mundo. En su nivel más elemental, una "cadena de bloques" es un ledger descentralizado y distribuido de transacciones digitales que permite un intercambio de dinero o datos sin confianza. En los modelos de pago existentes, como las transacciones con tarjeta de crédito, giro postal o electrónicas (por ejemplo, PayPal), existe un intermediario externo para facilitar el intercambio. Dentro de una transacción tradicional, la presencia de una institución centralizada, con incentivos financieros inherentes, introduce la posibilidad de sesgo, deshonestidad y, en última instancia, fraude. Además, incluso con las tecnologías financieras actuales, los procesos ineficientes de verificación transaccional pueden tardar días antes de que el dinero se retire de una cuenta y se deposite en otra. Teniendo en cuenta estos inconvenientes de los instrumentos financieros contemporáneos, la tecnología blockchain se ha desarrollado con el tiempo para abordar los problemas fundamentales de la confianza transaccional, la velocidad y la integridad.

Inicialmente descrita en 2009 por el individuo o grupo anónimo conocido como Satoshi Nakamoto, la cadena de bloques de Bitcoin se desarrolló como un sistema de efectivo electrónico peer-to-peer [10]. La cadena de bloques funciona agregando secuencialmente bloques cifrados de transacciones a una cadena y distribuyendo simultáneamente la cadena actualizada a nodos específicos a través de una red. Por lo tanto, dado que la cadena de bloques actualizada se distribuye de manera confiable, las transacciones dentro de los bloques individuales son inmutables y se puede verificar la integridad de la cadena de bloques. Las claves de identificación públicas se utilizan entre individuos en una transacción, y el pagador firma criptográficamente las transacciones utilizando una clave privada oculta, conocida solo por el pagador. Los mineros dentro de una cadena de bloques son nodos que construyen bloques de transacciones que se agregarán a la cadena y se les incentiva a trabajar mediante el cobro de tarifas de transacción. Por lo tanto, es a través de los mineros que se construye una cadena de bloques de consenso y se distribuye al resto de la red.

Desde el origen de Bitcoin, han surgido otras criptomonedas competidoras, cada una con un ledger único distribuido de transacciones, pero basado en una estructura de código blockchain variable. Algunas tecnologías de blockchain, como Ethereum, permiten que el espacio en bloques incluya "contratos inteligentes", o líneas de código que definen cláusulas autoejecutables y / o autoejecutables, que se ejecutan solo si se cumplen ciertas condiciones. La mayoría de las plataformas tienen tokens propiedad del usuario que se pueden usar para pagar costos de transacción, codificar contratos inteligentes o transferir datos entre individuos en la cadena de bloques. A medida que estas tecnologías han desarrollado un valor significativo en los últimos años, las nuevas plataformas pueden usar una "Oferta Inicial de Monedas (ICO)" para obtener financiamiento temprano. Estas monedas se pueden negociar públicamente en intercambios de criptomonedas, un enigmático sector financiero que tenía una capitalización de mercado de más de \$ 800 mil millones en enero de 2018 [8]. Sin embargo, desde que alcanzaron su punto máximo de valor en enero de 2018, los intercambios de criptomonedas han perdido aproximadamente el 80% de su valor, lo que refleja la sobrevaloración ante la lenta adopción por parte de varias industrias económicas [11].

En cualquier caso, el principio fundamental de una cadena de bloques, principalmente el libro mayor anónimo y distribuido de transacciones, sigue siendo relevante y aún se presta a ciertas aplicaciones tecnológicas, como el almacenamiento distribuido en la nube, la identificación digital cifrada y las estrategias de pago descentralizadas. Aquí, los paralelismos entre la tecnología blockchain y las necesidades centrales de la infraestructura moderna de atención médica son evidentes [4, 6, 13]. En la siguiente sección, revisamos varias soluciones potenciales que las tecnologías blockchain abordan en el panorama actual de TI de salud.

LIMITACIONES DE LA BLOCKCHAIN EN EL CUIDADO DE LA SALUD

El beneficio fundamental de una infraestructura blockchain es su registro compartido y no modificable de transacciones. Sin embargo, el hecho de que los datos se compartan entre todos los participantes en una red puede parecer socavar el anonimato necesario de la información de salud protegida (PHI). Esto se puede

abordar incorporando solo datos no identificados y cifrados en la cadena de bloques. Mientras que la información en la cadena de bloques en sí es pública, la PHI almacenada en repositorios de datos fuera de la cadena de bloques estaría fuertemente protegida y cumpliría con HIPAA. Una vez más, el acceso a estos datos solo sería permisible por el paciente, utilizando contratos inteligentes y una clave privada anónima para limitar el acceso solo a médicos específicos. La administración de esta clave privada puede resultar difícil para el paciente individual, especialmente para la población anciana o discapacitada, pero la vinculación biométrica precisa a la clave puede obviar un registro físico. Además, mantener una clave privada confidencial no es diferente de proteger un número de seguro social o un número de registro médico institucional para el acceso a datos médicos. La verdadera fortaleza de la tecnología blockchain radica en su capacidad para confirmar con total certeza que se ha producido una transacción o un evento, sin comprometer la información específica del evento.

El intercambio de datos distribuidos requiere una red de nodos para construir y mantener la cadena de bloques. Esto plantea dos problemas. En primer lugar, la creación de una red de atención médica de este tipo requiere una aceptación significativa de la comunidad médica. Los sistemas médicos existentes preservan el status quo, y una nueva infraestructura de atención médica puede resultar demasiado costosa o difícil para una implementación generalizada. En segundo lugar, mantener una red blockchain requiere una potencia informática significativa, lo que puede conducir a un mayor costo de hardware y consumo de energía por parte de un sistema hospitalario. En ambos casos, incentivar a los participantes en la cadena de bloques de atención médica puede conducir a su mayor utilización. Las aplicaciones basadas en blockchain pueden distribuir tokens a los participantes en la red, que se pueden intercambiar por servicios como un mayor almacenamiento de datos, una transferencia de datos más rápida o el acceso a un repositorio de datos. Los tokens también se pueden intercambiar por Bitcoin o dólares estadounidenses en un intercambio de criptomonedas, lo que permite la opción de compensación financiera directa.

Por último, tal como están ahora, los datos médicos privados están altamente protegidos tanto por el individuo como por su institución médica. Al reclamar la propiedad de una gran cantidad de registros de salud, los hospitales y las prácticas monetizan el intercambio de datos con investigadores y socios de la industria (por ejemplo, ensayos clínicos y estudios de salud pública). El movimiento hacia el almacenamiento y la distribución de datos descentralizados en una cadena de bloques puede encontrar un retroceso significativo por parte de las instituciones que valoran la propiedad de datos médicos. Cambiar fundamentalmente la propiedad de los registros de salud personales al paciente requerirá un cambio de paradigma filosófico tanto en la política de salud como en la ley.

CONCLUSIONES

En los próximos años, habrá avances revolucionarios en la infraestructura de TI de salud global. Las tecnologías emergentes servirán para abordar los problemas con el sistema actual, incluida la falta de interoperabilidad del software de registro electrónico de salud (EHR), la transferencia ineficiente e insegura de información de salud protegida (PHI), un sistema de pago ineficaz para la atención basada en el valor y la necesidad cambiante de atención centrada en el paciente. Crear e implementar una red de atención médica basada en blockchain puede abordar estos problemas de una manera revolucionaria. A medida que se desarrollan nuevas tecnologías, depende de los médicos mantener una actitud de aceptación, pero inquisitiva, una voluntad de implementar nuevas ideas y una filosofía de retroalimentación en lugar de un rechazo absoluto.

TRANSLATED VERSION: FRENCH

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

VERSION TRADUITE: FRANÇAIS

Voici une traduction approximative des idées présentées ci-dessus. Cela a été fait pour donner une compréhension générale des idées présentées dans le document. Veuillez excuser toutes les erreurs grammaticales et ne pas tenir les auteurs originaux responsables de ces erreurs.

INTRODUCTION

En janvier 2015, le président Barack Obama a adopté l'Initiative de médecine de précision, qui visait à « permettre une nouvelle ère de la médecine grâce à la recherche, à la technologie et aux politiques qui permettent aux patients, aux chercheurs et aux fournisseurs de travailler ensemble au développement de soins individualisés » [16]. Avec une attention accrue portée au traitement des patients individuels et non de leurs processus pathologiques, vient le besoin fondamental de données cliniques précises qui peuvent être largement distribuées aux prestataires de soins de santé de manière efficace et sécurisée. Bien que l'utilisation obligatoire des DSE ait été établie par le biais des critères d'utilisation significative des Centers for Medicare and Medicaid Services (CMS) des États-Unis en 2009 [1], le large éventail de DSE économiquement concurrents utilisés dans différents systèmes hospitaliers limite considérablement l'interopérabilité et empêche l'échange fluide d'informations sur la santé entre les établissements. Par conséquent, le dossier médical individuel d'un patient peut être considérablement fragmenté dans l'ensemble du système de santé, avec des documents importants tels que les antécédents médicaux, la liste des médicaments et les directives préalables potentiellement indisponibles dans les situations d'urgence.

À l'ère moderne des technologies de l'information, une quantité croissante de données est transmise et stockée sur des réseaux basés sur le cloud. Tel que défini par le National Institute of Standards and Technology (NIST) des États-Unis [9], le cloud computing est « un modèle permettant un accès réseau omniprésent, pratique et à la demande à un pool partagé de ressources informatiques configurables ». Le cloud computing s'est avéré idéal pour des services Internet tels que le partage d'informations, la sauvegarde de fichiers et l'analyse de données volumineuses, où la rentabilité et l'utilisation optimale des ressources sont essentielles. Ainsi, compte tenu des grandes quantités d'informations médicales générées quotidiennement, il y a eu une poussée récente vers le stockage et la distribution de données de soins de santé basés sur le cloud. Cependant, un référentiel de données centralisé et partagé présente un risque de violation de la cybersécurité et remet directement en question le droit individuel d'un patient à la vie privée.

C'est là que réside la complexité de la conception d'un système d'information sur la santé fonctionnel qui maintient toujours les principes fondamentaux d'un dossier médical, principalement l'exhaustivité, l'accessibilité, l'interopérabilité, la confidentialité, la responsabilité et la flexibilité [7]. En 2014, l'Office of the National Coordinator for Health Information Technology (ONC) des États-Unis a présenté sa vision sur 10 ans visant à mettre en place une infrastructure informatique universelle pour la santé [14], déclarant que « cet objectif ne sera possible qu'avec un écosystème informatique de santé solide et flexible qui peut soutenir de manière appropriée la transparence et la prise de décision, réduire les redondances, éclairer la réforme des paiements et aider à transformer les soins en un modèle qui améliore l'accès et aborde véritablement la santé au-delà des limites de la santé. système de soins. Le fondement d'un nouveau système de technologie de l'information sur les soins de santé doit être ancré dans l'interopérabilité des plateformes, de sorte que le stockage et l'accès aux données soient normalisés, que la sécurité et la confidentialité des patients soient prioritaires et qu'un dévouement aux soins centrés sur le patient soit maintenu.

TECHNOLOGIE BLOCKCHAIN

Récemment, l'accent a été mis sur le développement de technologies basées sur la blockchain dans le monde entier. À son niveau le plus élémentaire, une « blockchain » est un léger décentralisé et distribué de transactions numériques qui permet un échange sans confiance d'argent ou de données. Dans les modèles de paiement existants, tels que les transactions par carte de crédit, mandat ou électronique (par exemple, PayPal), un intermédiaire tiers existe pour faciliter l'échange. Dans une transaction traditionnelle, la

présence d'une institution centralisée, avec des incitations financières inhérentes, introduit la possibilité de partialité, de malhonnêteté et, en fin de compte, de fraude. De plus, même avec les technologies financières actuelles, les processus inefficaces de vérification transactionnelle peuvent prendre des jours avant que l'argent ne soit retiré d'un compte et déposé dans un autre. Compte tenu de ces inconvénients des instruments financiers contemporains, la technologie blockchain s'est développée au fil du temps pour résoudre les problèmes fondamentaux de la confiance, de la rapidité et de l'intégrité des transactions.

Initialement décrite en 2009 par l'individu ou le groupe anonyme connu sous le nom de Satoshi Nakamoto, la blockchain Bitcoin a été développée comme un système de paiement électronique peer-to-peer [10]. La blockchain fonctionne en ajoutant séquentiellement des blocs de transactions cryptés à une chaîne et en distribuant simultanément la chaîne mise à jour à des nœuds spécifiés sur un réseau. Ainsi, puisque la blockchain mise à jour est distribuée de manière fiable, les transactions au sein des blocs individuels sont immuables et l'intégrité de la blockchain peut être vérifiée. Les clés d'identification publiques sont utilisées entre les personnes dans une transaction, et le payeur signe cryptographiquement les transactions à l'aide d'une clé privée cachée, connue uniquement du payeur. Les mineurs au sein d'une blockchain sont des nœuds qui construisent des blocs de transactions à ajouter à la chaîne et sont incités à travailler en collectant des frais de transaction. Ainsi, c'est à travers les mineurs qu'une blockchain consensuelle est construite et distribuée au reste du réseau.

Depuis l'origine de Bitcoin, d'autres crypto-monnaies concurrentes ont émergé, chacune avec un léger distribué unique de transactions, mais basé sur une structure de code blockchain variable. Certaines technologies blockchain, telles que Ethereum, permettent à l'espace dans les blocs d'inclure des « contrats intelligents », ou des lignes de code qui définissent des clauses auto-exécutables et / ou auto-exécutaires, ne s'exécutant que si certaines conditions sont remplies. La plupart des plates-formes ont des jetons appartenant aux utilisateurs qui peuvent être utilisés pour payer les coûts de transaction, encoder des contrats intelligents ou transférer des données entre individus sur la blockchain. Comme ces technologies ont développé une valeur significative ces dernières années, les nouvelles plates-formes peuvent utiliser une « offre initiale de pièces de monnaie (ICO) » pour obtenir un financement précoce. Ces pièces peuvent être cotées en bourse sur les bourses de crypto-monnaie, un secteur financier énigmatique qui avait une capitalisation boursière de plus de 800 milliards de dollars en janvier 2018 [8]. Depuis le pic de valeur atteint en janvier 2018, cependant, les échanges de crypto-monnaie ont perdu environ 80% de leur valeur, reflétant une surévaluation face à la lente adoption par diverses industries économiques [11].

Quoi qu'il en soit, le principe fondamental d'une blockchain, principalement le registre anonyme et distribué des transactions, reste pertinent et se prête toujours à certaines applications technologiques, telles que le stockage en nuage distribué, l'identification numérique cryptée et les stratégies de paiement décentralisées. Ici, les parallèles entre la technologie blockchain et les besoins fondamentaux de l'infrastructure moderne des soins de santé sont évidents [4, 6, 13]. Dans la section suivante, nous passons en revue plusieurs solutions potentielles que les technologies blockchain abordent dans le paysage informatique actuel de la santé.

LIMITES DE LA BLOCKCHAIN DANS LES SOINS DE SANTÉ

L'avantage fondamental d'une infrastructure blockchain est son enregistrement partagé et non modifiable des transactions. Cependant, le fait que les données soient partagées entre tous les participants d'un réseau peut sembler compromettre l'anonymat nécessaire des renseignements de santé protégés (RPS). Cela peut être résolu en incorporant uniquement des données anonymées et cryptées dans la blockchain. Alors que les informations de la blockchain elle-même sont publiques, les PHI stockés dans des référentiels de données hors de la blockchain seraient fortement protégés et conformes à la HIPPA. Encore une fois, l'accès à ces données ne serait autorisé que par le patient, en utilisant des contrats intelligents et une clé privée anonyme pour limiter l'accès aux seuls cliniciens spécifiés. La gestion de cette clé privée peut s'avérer difficile pour le patient individuel, en particulier pour les personnes âgées ou handicapées, mais un lien biométrique précis avec sa clé peut éviter un enregistrement physique. En outre, le maintien d'une clé privée confidentielle n'est pas différent de la protection d'un numéro de sécurité sociale ou d'un numéro

de dossier médical institutionnel pour l'accès aux données médicales. La véritable force de la technologie blockchain réside dans sa capacité à confirmer avec une certitude totale qu'une transaction ou un événement a eu lieu, sans compromettre les informations spécifiques de l'événement.

Le partage de données distribué nécessite un réseau de nœuds pour construire et maintenir la blockchain. Cela pose deux problèmes. Premièrement, la création d'un tel réseau de soins de santé nécessite une adhésion importante de la communauté médicale. Les systèmes médicaux existants préservent le statu quo, et une nouvelle infrastructure de soins de santé peut s'avérer trop coûteuse ou difficile pour une mise en œuvre à grande échelle. Deuxièmement, la maintenance d'un réseau blockchain nécessite une puissance de calcul importante, ce qui peut entraîner une augmentation du coût du matériel et de la consommation d'énergie par un système hospitalier. Dans les deux cas, inciter les participants à la blockchain des soins de santé peut conduire à une plus grande utilisation. Les applications basées sur la blockchain peuvent distribuer des jetons aux participants au réseau, qui peuvent être échangés contre des services tels qu'un stockage accru des données, un transfert de données plus rapide ou l'accès à un référentiel de données. Les jetons peuvent également être échangés contre des bitcoins ou des dollars américains sur un échange de crypto-monnaie, ce qui permet une compensation financière directe.

Enfin, dans l'état actuel des choses, les données médicales privées sont hautement protégées tant par l'individu que par son établissement médical. En revendiquant la propriété d'un grand nombre de dossiers de santé, les hôpitaux et les cabinets monétisent le partage de données avec les chercheurs et les partenaires de l'industrie (par exemple, les essais cliniques et les études de santé publique). Le mouvement vers le stockage et la distribution décentralisés des données sur une blockchain peut rencontrer un recul important de la part des institutions qui valorisent la propriété des données médicales. Transférer fondamentalement la propriété des dossiers de santé personnels au patient nécessitera un changement de paradigme philosophique à la fois dans la politique et la loi en matière de santé.

CONCLUSIONS

Dans les années à venir, il y aura des avancées révolutionnaires dans l'infrastructure informatique mondiale de la santé. Les technologies émergentes serviront à résoudre les problèmes liés au système actuel, notamment le manque d'interopérabilité des logiciels de dossiers de santé électroniques (DSE), le transfert inefficace et non sécurisé de renseignements de santé protégés (RPS), un système de paiement inefficace pour les soins fondés sur la valeur et le besoin changeant de soins centrés sur le patient. La création et la mise en œuvre d'un réseau de soins de santé basé sur la blockchain peuvent résoudre ces problèmes de manière révolutionnaire. Au fur et à mesure que de nouvelles technologies sont développées, il appartient aux cliniciens de maintenir une attitude tolérante, mais curieuse, une volonté de mettre en œuvre de nouvelles idées et une philosophie de rétroaction plutôt que de rejet absolu.

TRANSLATED VERSION: GERMAN

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

ÜBERSETZTE VERSION: DEUTSCH

Hier ist eine ungefähre Übersetzung der oben vorgestellten Ideen. Dies wurde getan, um ein allgemeines Verständnis der in dem Dokument vorgestellten Ideen zu vermitteln. Bitte entschuldigen Sie alle grammatikalischen Fehler und machen Sie die ursprünglichen Autoren nicht für diese Fehler verantwortlich.

EINLEITUNG

Im Januar 2015 erließ Präsident Barack Obama die Precision Medicine Initiative, die darauf abzielte, "eine neue Ära der Medizin durch Forschung, Technologie und Richtlinien zu ermöglichen, die Patienten, Forscher und Anbieter befähigen, gemeinsam auf die Entwicklung einer individualisierten Versorgung hinzuarbeiten" [16]. Mit einem verstärkten Fokus auf die Behandlung einzelner Patienten und nicht auf ihre Krankheitsprozesse entsteht der grundlegende Bedarf an genauen klinischen Daten, die auf effiziente und sichere Weise an Gesundheitsdienstleister verteilt werden können. Obwohl die obligatorische Verwendung von EHRs über die Meaningful Use-Kriterien der US-amerikanischen Centers for Medicare and Medicaid Services (CMS) im Jahr 2009 [1] festgelegt wurde, schränkt die breite Palette wirtschaftlich konkurrierender EHRs, die in verschiedenen Krankenhaussystemen verwendet werden, die Interoperabilität erheblich ein und verhindert den fließenden Austausch von Gesundheitsinformationen zwischen Institutionen. Infolgedessen kann die individuelle Krankenakte eines Patienten im gesamten Gesundheitssystem erheblich fragmentiert sein, wobei wichtige Dokumente wie Krankengeschichte, Medikamentenliste und Patientenverfügungen in Notfallsituationen möglicherweise nicht verfügbar sind.

Im modernen Zeitalter der Informationstechnologie werden immer mehr Daten in Cloud-basierten Netzwerken übertragen und gespeichert. Wie vom US-amerikanischen National Institute of Standards and Technology (NIST) [9] definiert, ist Cloud Computing "ein Modell, um einen allgegenwärtigen, bequemen On-Demand-Netzwerkzugriff auf einen gemeinsamen Pool konfigurierbarer Computerressourcen zu ermöglichen". Cloud Computing hat sich als ideal für Internetdienste wie Informationsaustausch, Datensicherung und Big Data-Analysen erwiesen, bei denen Kosteneffizienz und optimale Ressourcennutzung unerlässlich sind. Angesichts der riesigen Mengen an medizinischen Informationen, die täglich generiert werden, gab es in letzter Zeit einen Schub in Richtung Cloud-basierter Speicherung und Verteilung von Gesundheitsdaten. Ein zentralisiertes, gemeinsam genutztes Daten-Repository birgt jedoch das Risiko einer Cybersicherheitsverletzung und stellt das individuelle Recht eines Patienten auf Privatsphäre direkt in Anspruch.

Hierin liegt die Komplexität der Gestaltung eines funktionalen Gesundheitsinformationssystems, das immer noch die Kernprinzipien einer Krankenakte beibehält, hauptsächlich Vollständigkeit, Zugänglichkeit, Interoperabilität, Vertraulichkeit, Rechenschaftspflicht und Flexibilität [7]. Im Jahr 2014 präsentierte das U.S. Office of the National Coordinator for Health Information Technology (ONC) seine 10-Jahres-Vision zur Erreichung einer universellen IT-Infrastruktur für das Gesundheitswesen [14] und erklärte, dass "dieses Ziel nur mit einem starken, flexiblen Gesundheits-IT-Ökosystem möglich sein wird, das Transparenz und Entscheidungsfindung angemessen unterstützen, Redundanzen reduzieren, Zahlungsreformen informieren und dazu beitragen kann, die Pflege in ein Modell zu verwandeln, das den Zugang verbessert und die Gesundheit über die Grenzen der Gesundheit hinaus wirklich anspricht Pflegesystem." Die Grundlage eines neuen Informationstechnologiesystems für das Gesundheitswesen muss in der Plattforminteroperabilität verwurzelt sein, so dass Datenspeicherung und -zugriff standardisiert sind, Patientensicherheit und Vertraulichkeit Priorität haben und ein Engagement für eine patientenzentrierte Versorgung aufrechterhalten wird.

BLOCKCHAIN-TECHNOLOGIE

In letzter Zeit wurde der Schwerpunkt intensiv auf die Entwicklung von Blockchain-basierten Technologien auf der ganzen Welt gerichtet. Auf ihrer elementarsten Ebene ist eine "Blockchain" ein dezentraler, verteilter Ledger digitaler Transaktionen, der einen vertrauenslosen Austausch von Geld oder Daten ermöglicht. In bestehenden Zahlungsmodellen wie Kreditkarte, Zahlungsanweisung oder elektronischen (z. B. PayPal) Transaktionen existiert ein externer Vermittler, um den Austausch zu erleichtern. Innerhalb einer traditionellen Transaktion führt die Anwesenheit einer zentralisierten Institution mit inhärenten finanziellen Anreizen zu der Möglichkeit von Voreingenommenheit, Unehrlichkeit und letztendlich Betrug. Darüber hinaus können selbst mit aktuellen Finanztechnologien die ineffizienten Prozesse der Transaktionsüberprüfung Tage dauern, bevor Geld von einem Konto abgeboben und auf ein

anderes eingezahlt wird. In Anbetracht dieser Nachteile zeitgenössischer Finanzinstrumente hat sich die Blockchain-Technologie im Laufe der Zeit entwickelt, um die grundlegenden Probleme des transaktionalen Vertrauens, der Geschwindigkeit und der Integrität anzugehen.

Ursprünglich im Jahr 2009 von der anonymen Person oder Gruppe Satoshi Nakamoto beschrieben, wurde die Bitcoin-Blockchain als Peer-to-Peer-Electronic-Cash-System entwickelt [10]. Die Blockchain funktioniert, indem sie einer Kette sequenziell verschlüsselte Transaktionsblöcke hinzufügt und gleichzeitig die aktualisierte Kette an bestimmte Knoten über ein Netzwerk verteilt. Da also die aktualisierte Blockchain zuverlässig verteilt ist, sind die Transaktionen innerhalb der einzelnen Blöcke unveränderlich und die Integrität der Blockchain kann überprüft werden. Öffentliche Identifikationsschlüssel werden zwischen Einzelpersonen in einer Transaktion verwendet, und der Zahler signiert Transaktionen kryptografisch mit einem versteckten privaten Schlüssel, der nur dem Zahler bekannt ist. Miner innerhalb einer Blockchain sind Knoten, die Blöcke von Transaktionen konstruieren, die der Kette hinzugefügt werden sollen, und die durch das Sammeln von Transaktionsgebühren dazu anregen, zu arbeiten. So wird durch die Miner eine Konsens-Blockchain aufgebaut und an den Rest des Netzwerks verteilt.

Seit dem Ursprung von Bitcoin sind andere konkurrierende Kryptowährungen entstanden, jede mit einem einzigartigen verteilten Transaktionsspiel, das jedoch auf einer variablen Blockchain-Codestruktur basiert. Einige Blockchain-Technologien, wie Ethereum, erlauben Platz in Blöcken, um "Smart Contracts" oder Codezeilen zu enthalten, die selbstaufführende und / oder selbsterzwingende Klauseln definieren, die nur ausgeführt werden, wenn bestimmte Bedingungen erfüllt sind. Die meisten Plattformen verfügen über benutzereigene Token, mit denen Transaktionskosten bezahlt, Intelligente Verträge codiert oder Daten zwischen Personen in der Blockchain übertragen werden können. Da diese Technologien in den letzten Jahren einen erheblichen Wert entwickelt haben, können neue Plattformen ein "Initial Coin Offering (ICO)" nutzen, um eine frühzeitige Finanzierung zu erhalten. Diese Münzen können öffentlich an Kryptowährungsbörsen gehandelt werden, einem rätselhaften Finanzsektor, der im Januar 2018 eine Marktkapitalisierung von über 800 Milliarden US-Dollar hatte [8]. Seit dem Höhepunkt des Wertes im Januar 2018 haben Kryptowährungsbörsen jedoch etwa 80% ihres Wertes verloren, was auf eine Überbewertung angesichts der langsamen Akzeptanz durch verschiedene Wirtschaftssektoren zurückzuführen ist [11].

Unabhängig davon bleibt das Grundprinzip einer Blockchain, hauptsächlich das anonyme, verteilte Transaktionsbuch, relevant und eignet sich immer noch für bestimmte technologische Anwendungen wie verteilte Cloud-Speicherung, verschlüsselte digitale Identifizierung und dezentrale Zahlungsstrategien. Hier zeigen sich die Parallelen zwischen der Blockchain-Technologie und den Kernbedürfnissen der modernen Gesundheitsinfrastruktur [4, 6, 13]. Im folgenden Abschnitt werden einige potenzielle Lösungen erläutert, die Blockchain-Technologien in der aktuellen IT-Landschaft im Gesundheitswesen adressieren.

GRENZEN DER BLOCKCHAIN IM GESUNDHEITSWESEN

Der grundlegende Vorteil einer Blockchain-Infrastruktur ist ihre gemeinsame, nicht veränderbare Aufzeichnung von Transaktionen. Die Tatsache, dass Daten zwischen allen Teilnehmern eines Netzwerks ausgetauscht werden, scheint jedoch die notwendige Anonymität geschützter Gesundheitsinformationen (PHI) zu untergraben. Dies kann behoben werden, indem nur anonymisierte und verschlüsselte Daten in die Blockchain integriert werden. Während Informationen in der Blockchain selbst öffentlich sind, wäre PHI, das in Datenrepositorien außerhalb der Blockchain gespeichert ist, stark geschützt und HIPPA-konform. Auch hier wäre der Zugriff auf diese Daten nur für den Patienten zulässig, indem er intelligente Verträge und einen anonymen privaten Schlüssel verwendet, um den Zugriff nur auf bestimmte Kliniker zu beschränken. Die Verwaltung dieses privaten Schlüssels kann sich für den einzelnen Patienten, insbesondere für ältere oder behinderte Menschen, als schwierig erweisen, aber eine genaue biometrische Verknüpfung mit dem eigenen Schlüssel kann eine physische Aufzeichnung erleichtern. Darüber hinaus unterscheidet sich die Pflege eines vertraulichen privaten Schlüssels nicht vom Schutz einer Sozialversicherungsnummer oder einer institutionellen Krankenaktennummer für den Zugriff auf medizinische Daten. Die wahre Stärke der Blockchain-Technologie liegt in ihrer Fähigkeit, mit absoluter

Sicherheit zu bestätigen, dass eine Transaktion oder ein Ereignis stattgefunden hat, ohne die spezifischen Informationen des Ereignisses zu beeinträchtigen.

Die verteilte Gemeinsame Nutzung von Daten erfordert ein Netzwerk von Knoten, um die Blockchain aufzubauen und zu warten. Dies wirft zwei Probleme auf. Erstens erfordert die Schaffung eines solchen Gesundheitsnetzwerks eine erhebliche Buy-in-Community der medizinischen Gemeinschaft. Bestehende medizinische Systeme bewahren den Status quo, und eine neuartige Gesundheitsinfrastruktur kann sich für eine breite Implementierung als zu teuer oder schwierig erweisen. Zweitens erfordert die Wartung eines Blockchain-Netzwerks eine erhebliche Rechenleistung, die zu höheren Kosten für Hardware und Energieverbrauch durch ein Krankenhaussystem führen kann. In beiden Fällen kann die Anreize für Teilnehmer an der Blockchain im Gesundheitswesen zu einer höheren Nutzung führen. Blockchain-basierte Anwendungen können Token an Teilnehmer im Netzwerk verteilen, die gegen Dienste wie erhöhte Datenspeicherung, schnellere Datenübertragung oder Zugriff auf ein Datenrepository ausgetauscht werden können. Token können auch für Bitcoin oder US-Dollar an einer Kryptowährungsbörse gehandelt werden, was die Option für eine direkte finanzielle Entschädigung ermöglicht.

Schließlich sind private medizinische Daten sowohl vom Einzelnen als auch von seiner medizinischen Einrichtung in hohem Maße geschützt. Durch die Beanspruchung des Eigentums an einer großen Menge an Gesundheitsakten monetarisieren Krankenhäuser und Praxen den Datenaustausch mit Forschern und Industriepartnern (z. B. klinische Studien und Studien zur öffentlichen Gesundheit). Die Bewegung hin zu einer dezentralen Datenspeicherung und -verteilung auf einer Blockchain kann von Institutionen, die wertschätzen, auf das Eigentum an medizinischen Daten zurückgedrängt werden. Die grundlegende Verlagerung des Eigentums an persönlichen Gesundheitsakten auf den Patienten erfordert einen philosophischen Paradigmenwechsel sowohl in der Gesundheitspolitik als auch im Recht.

SCHLÜSSE

In den kommenden Jahren wird es revolutionäre Fortschritte in der globalen Gesundheits-IT-Infrastruktur geben. Neue Technologien werden dazu dienen, Probleme mit dem derzeitigen System anzugehen, einschließlich der mangelnden Interoperabilität der Software für elektronische Patientenakten (EHR), der ineffizienten und unsicheren Übertragung geschützter Gesundheitsinformationen (PHI), eines ineffektiven Zahlungssystems für eine wertorientierte Versorgung und des sich entwickelnden Bedarfs an patientenzentrierter Versorgung. Die Schaffung und Implementierung eines Blockchain-basierten Gesundheitsnetzwerks kann diese Probleme auf revolutionäre Weise angehen. Bei der Entwicklung neuartiger Technologien liegt es an den Klinikern, eine akzeptierende, aber neugierige Haltung, die Bereitschaft, neue Ideen umzusetzen, und eine Philosophie des Feedbacks und nicht der absoluten Ablehnung beizubehalten.

TRANSLATED VERSION: PORTUGUESE

Below is a rough translation of the insights presented above. This was done to give a general understanding of the ideas presented in the paper. Please excuse any grammatical mistakes and do not hold the original authors responsible for these mistakes.

VERSÃO TRADUZIDA: PORTUGUÊS

Aqui está uma tradução aproximada das ideias acima apresentadas. Isto foi feito para dar uma compreensão geral das ideias apresentadas no documento. Por favor, desculpe todos os erros gramaticais e não responsabilize os autores originais responsáveis por estes erros.

INTRODUÇÃO

Em janeiro de 2015, o presidente Barack Obama promulgou a Iniciativa de Medicina de Precisão, que visava "viabilizar uma nova era da medicina por meio de pesquisas, tecnologia e políticas que capacitem pacientes, pesquisadores e provedores a trabalhar em conjunto para o desenvolvimento do cuidado individualizado" [16]. Com um foco intensificado no tratamento de pacientes individuais e não em seus processos de doença, vem a necessidade fundamental de dados clínicos precisos que possam ser amplamente distribuídos aos profissionais de saúde de forma eficiente e segura. Embora o uso obrigatório de EHRs tenha sido estabelecido através dos critérios de Uso Significativo dos Centros de Assistência Médica e Medicaid (CMS) dos EUA em 2009 [1], a ampla gama de EHRs economicamente concorrentes usados em diferentes sistemas hospitalares limita significativamente a interoperabilidade e impede a troca fluida de informações de saúde entre as instituições. Como resultado, o prontuário individual de um paciente pode ser significativamente fragmentado em todo o sistema de saúde, com documentos importantes como histórico médico, lista de medicamentos e diretrizes avançadas potencialmente indisponíveis em situações de emergência.

Na era moderna da tecnologia da informação, uma quantidade crescente de dados está sendo transmitida e armazenada em redes baseadas em nuvem. Conforme definido pelo Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) [9], a computação em nuvem é "um modelo para permitir acesso onipresente, conveniente e sob demanda a um pool compartilhado de recursos computacionais configuráveis". A computação em nuvem tem se mostrado ideal para serviços de Internet como compartilhamento de informações, backup de arquivos e análise de big data, onde o custo-efetividade e a utilização ideal de recursos são essenciais. Assim, dadas as vastas quantidades de informações médicas geradas diariamente, houve um recente impulso para o armazenamento e distribuição de dados de cuidados de saúde baseados em nuvem. No entanto, um repositório de dados centralizado e compartilhado apresenta o risco de violação da segurança cibernética e desafia diretamente o direito individual do paciente à privacidade.

Aqui reside a complexidade de projetar um sistema funcional de informação em saúde que ainda mantém os princípios fundamentais de um prontuário médico, principalmente integralidade, acessibilidade, interoperabilidade, confidencialidade, prestação de contas e flexibilidade [7]. Em 2014, o Escritório da Coordenadoria Nacional de Tecnologia da Informação em Saúde (ONC) apresentou sua visão de 10 anos para alcançar uma infraestrutura universal de TI em Saúde [14], afirmando que "esse objetivo só será possível com um ecossistema de TI de saúde forte e flexível que possa apoiar adequadamente a transparência e a tomada de decisões, reduzir a redundância, informar a reforma de pagamentos e ajudar a transformar o cuidado em um modelo que melhore o acesso e realmente atenda à saúde além dos limites da saúde além dos limites da saúde sistema de cuidados. A fundação de um novo sistema de tecnologia da informação em saúde deve estar enraizada na interoperabilidade da plataforma, de tal forma que o armazenamento e o acesso de dados são padronizados, a segurança e a confidencialidade do paciente são priorizados e uma dedicação ao cuidado centrado no paciente é mantida.

TECNOLOGIA BLOCKCHAIN

Recentemente, houve um intenso foco no desenvolvimento de tecnologias baseadas em blockchain em todo o mundo. Em seu nível mais elementar, um "blockchain" é um ledger descentralizado e distribuído de transações digitais que permite uma troca de dinheiro ou dados sem confiança. Nos modelos de pagamento existentes, como cartão de crédito, ordem monetária ou transações eletrônicas (ex. PayPal), existe um intermediário de terceiros para facilitar a troca. Dentro de uma transação tradicional, a presença de uma instituição centralizada, com incentivos financeiros inerentes, introduz a possibilidade de viés, desonestidade e, em última instância, fraude. Além disso, mesmo com as tecnologias financeiras vigentes, os processos ineficientes de verificação transacional podem levar dias até que o dinheiro seja retirado de uma conta e depositado em outra. Considerando essas desvantagens aos instrumentos financeiros contemporâneos, a tecnologia blockchain desenvolveu-se ao longo do tempo para resolver os problemas fundamentais da confiança transacional, velocidade e integridade.

Inicialmente descrito em 2009 pelo indivíduo anônimo ou grupo conhecido como Satoshi Nakamoto, o blockchain Bitcoin foi desenvolvido como um sistema de caixa eletrônico peer-to-peer [10]. O blockchain funciona adicionando sequencialmente blocos criptografados de transações a uma cadeia e distribuindo simultaneamente a cadeia atualizada para nós especificados em uma rede. Assim, uma vez que o blockchain atualizado é distribuído de forma confiável, as transações dentro dos blocos individuais são imutáveis, e a integridade do blockchain pode ser verificada. As chaves de identificação pública são usadas entre indivíduos em uma transação, e o pagador assina criptograficamente transações usando uma chave privada escondida, conhecida apenas pelo pagador. Os mineradores dentro de um blockchain são nós que constroem blocos de transações a serem adicionados à cadeia, e são incentivados a trabalhar coletando taxas de transação. Assim, é através dos mineradores que um blockchain de consenso é construído e distribuído para o resto da rede.

Desde a origem do Bitcoin, outras criptomoedas concorrentes surgiram, cada uma com um ledger distribuído único de transações, mas com base em uma estrutura de código blockchain variável. Algumas tecnologias blockchain, como o Ethereum, permitem que o espaço em blocos inclua "contratos inteligentes", ou linhas de código que definem cláusulas de auto-execução e/ou auto-execução, funcionando apenas se determinadas condições forem atendidas. A maioria das plataformas possui tokens de propriedade do usuário que podem ser usados para pagar custos de transação, codificar contratos inteligentes ou transferir dados entre indivíduos na blockchain. Como essas tecnologias desenvolveram um valor significativo nos últimos anos, novas plataformas podem usar uma "Oferta Inicial de Moedas (ICO)" para obter financiamento antecipado. Essas moedas podem ser negociadas publicamente em exchanges de criptomoedas, um setor financeiro enigmático que teve uma capitalização de mercado de mais de US \$ 800 bilhões em janeiro de 2018 [8]. Desde o pico de valor em janeiro de 2018, no entanto, as exchanges de criptomoedas perderam aproximadamente 80% de seu valor, refletindo a supervalorização diante da lenta adoção por várias indústrias econômicas [11].

Independentemente disso, o princípio fundamental de um blockchain, principalmente o livro anônimo e distribuído de transações, permanece relevante e ainda se presta a certos aplicativos tecnológicos, como armazenamento distribuído em nuvem, identificação digital criptografada e estratégias de pagamento descentralizadas. Aqui, os paralelos entre a tecnologia blockchain e as necessidades centrais da moderna infraestrutura de saúde são aparentes [4, 6, 13]. Na seção seguinte, revisamos várias soluções potenciais que as tecnologias blockchain abordam no atual cenário de TI em saúde.

LIMITAÇÕES DO BLOCKCHAIN NA ÁREA DA SAÚDE

O benefício fundamental de uma infraestrutura blockchain é seu registro compartilhado e não modificável de transações. No entanto, o fato de os dados serem compartilhados entre todos os participantes de uma rede pode parecer minar o anonimato necessário das informações de saúde protegidas (PHI). Isso pode ser resolvido incorporando apenas dados não identificados e criptografados no blockchain. Considerando que as informações no blockchain em si são públicas, o PHI armazenado em repositórios de dados fora do blockchain estaria fortemente protegido e compatível com HIPAA. Mais uma vez, o acesso a esses dados só seria permitido pelo paciente, utilizando contratos inteligentes e uma chave privada anônima para limitar o acesso apenas a médicos especificados. Gerenciar essa chave privada pode ser difícil para o paciente individual, especialmente para a população idosa ou deficiente, mas a ligação biométrica precisa à chave pode evitar um registro físico. Além disso, manter uma chave privada confidencial não é diferente de proteger um número de segurança social ou número de registro médico institucional para acesso a dados médicos. A verdadeira força da tecnologia blockchain está em sua capacidade de confirmar com total certeza que uma transação ou um evento ocorreu, sem comprometer as informações específicas do evento.

O compartilhamento distribuído de dados requer uma rede de nós para construir e manter o blockchain. Isso representa dois problemas. Em primeiro lugar, a criação dessa rede de saúde requer uma entrada significativa da comunidade médica. Os sistemas médicos existentes preservam o status quo, e uma nova infraestrutura de saúde pode ser muito cara ou difícil para a implementação generalizada. Em segundo lugar, a manutenção de uma rede blockchain requer um poder computacional significativo, o que pode levar

a um maior custo de consumo de hardware e energia por um sistema hospitalar. Em ambos os casos, incentivar os participantes na blockchain da saúde pode levar a uma maior utilização. Os aplicativos baseados em blockchain podem distribuir tokens aos participantes da rede, que podem ser trocados por serviços como maior armazenamento de dados, transferência de dados mais rápida ou acesso a um repositório de dados. Os tokens também podem ser negociados por Bitcoin ou dólares americanos em uma bolsa de criptomoedas, permitindo a opção de compensação financeira direta.

Por fim, como está agora, os dados médicos privados são altamente protegidos tanto pelo indivíduo quanto por sua instituição médica. Ao reivindicar a propriedade sobre uma grande quantidade de registros de saúde, hospitais e práticas monetizam o compartilhamento de dados com pesquisadores e parceiros da indústria (ex. ensaios clínicos e estudos de saúde pública). O movimento para o armazenamento e distribuição descentralizados de dados em uma blockchain pode encontrar um recuo significativo por instituições que valorizam a propriedade de dados médicos. A mudança fundamental dos registros pessoais de saúde para o paciente exigirá uma mudança filosófica de paradigma tanto na política de saúde quanto na lei.

CONCLUSÕES

Nos próximos anos, haverá avanços revolucionários na infraestrutura global de TI em saúde. As tecnologias emergentes servirão para resolver problemas com o sistema atual, incluindo a falta de interoperabilidade do software de registro eletrônico de saúde (EHR), a transferência ineficiente e insegura das informações de saúde protegidas (PHI), um sistema de pagamento ineficaz para cuidados baseados em valor e a necessidade em evolução do cuidado centrado no paciente. Criar e implementar uma rede de saúde baseada em blockchain pode resolver esses problemas de forma revolucionária. À medida que novas tecnologias são desenvolvidas, cabe aos médicos manter uma atitude aceita, mas curiosa, uma vontade de implementar novas ideias e uma filosofia de feedback em vez de demissão absoluta.