Pragmatic, Interdisciplinary Perspectives on Blockchain and Distributed Ledger Technology: Paving the Future for Healthcare

Article · March 2018

DOI: 10.30953/bhty.v1.24

9 authors, including:

Ron Ribitzky
R&D Ribitzky
11 PUBLICATIONS **63** CITATIONS
SEE PROFILE

Brian Ahier
2 PUBLICATIONS **33** CITATIONS
SEE PROFILE

Kevin Clauson
Lipscomb University
98 PUBLICATIONS **2,072** CITATIONS
SEE PROFILE

BLOCKCHAIN™ IN HEALTHCARE TODAY

Pragmatic, Interdisciplinary Perspectives on Blockchain and Distributed Ledger Technology: Paving the Future for Healthcare

Ron Ribitzky,[1] James St. Clair,[2] David I. Houlding,[3] Chrissa T. McFarlane,[4] Brian Ahier,[5] Michael Gould,[6] Heather L. Flannery,[7] Erik Pupo,[8] Kevin A. Clauson[9]

Authors: [1]Ron Ribitzky, R&D Ribitzky, Newton, Massachusetts, U.S.A. [2]James St. Clair, Institute for Healthcare Financial Technology, Biloxi Mississippi, U.S.A.[3] David I. Houlding, Intel Health & Life Sciences, Santa Clara, California, U.S.A. [4]Chrissa T. McFarlane, Patientory, Atlanta, Georgia, U.S.A. [5] Brian Ahier, Aetna, Washington, DC, U.S.A. [6]Michael Gould, Independence Blue Cross, Philadelphia, Pennsylvania, U.S.A. [7]Heather L. Flannery, Obesity PPM, Washington, DC, U.S.A. [8]Erik Pupo, Accenture Health Client Service Group, Miami, Florida, U.S.A. [9]Kevin A. Clauson, Lipscomb University College of Pharmacy & Health Sciences, Nashville, Tennessee, USA.

Corresponding Author: Ron Ribitzky, R&D Ribitzky, 1929 Beacon Street, Newton, MA 02468 Ron@RDRibitzky.com, 617.599.2200

Keywords: Adoption, Blockchain, Global, Healthcare, Innovation, Interoperability

Section: Opinion/Perspective/Point of View

Background: *Blockchain and distributed ledger technology is a disruptive force in healthcare.*
Methods: *This article provides a globally relevant, interdisciplinary perspective intended to aid disparate group of actors, participants, and users that represent the diverse stakeholders of an increasingly complex and technologically reliant healthcare system. Domain expertise reinforced by literature published via industry, technical, and academic venues was used to inform these perspectives.*
Results: *Key characteristics of blockchain and distributed ledger technology are highlighted and framed for a readership ranging from healthcare executive to policy makers to researchers. Antecedent application of blockchain in the financial sector is explored followed by the technical, security, and interoperability considerations specific to healthcare.*
Conclusion: *Blockchain remains an emerging technology both fraught with unanticipated challenges and the promise of unrealized potential in healthcare.*

Keywords: Blockchain, Healthcare, Innovation, Adoption, Global, Interoperability

Blockchain technology is designed to establish trust, accountability, traceability, and integrity of data sharing. Leveraging these design goals to secure distributed data across traditional organizational and national boundaries is drawing enormous attention and resources around the world. Healthcare is no exception.[1-7]

Blockchain Characteristics

Blockchains are currently the most popular form of distributed ledger technology (DLT) being adopted today.[1-3] The foundational construct of blockchain, a DLT, is stored by each node in a 'permissionless' or public network (i.e., one that allows anyone to participate) or may be structured as a 'permissioned' or private network (i.e., whereby participation is controlled by the originator of the network).

For each block on the blockchain, a hash code is computed as a combination of the data in the block as well as the hash code of the previous block. In this way, hash codes are chained. Hash codes are easy to compute and verify by all participants of the blockchain, enabling them to verify the blockchain data has not been altered. Deletion of a block or changing the data on a block renders the chain of hash codes on the blockchain invalid and is easily detectable by the blockchain participants.

Each node, or network participant, continuously synchronizes the blockchain as consensus is achieved according to the specific consensus protocol of that network. This consensus ensures the validity and consistency of each copy of the distributed ledger running on each node of the blockchain network.

The data distribution model is a defining characteristic of the technology: centralized authorities do not communicate updates to records. Instead, each node executes peer-to-peer communication to trigger updates and achieve consensus among the nodes. Subject to the type of network (i.e., whether private or public), and the corresponding network design, certain nodes may or may not process some or all the transactions. Respectively, each processing node reaches its own conclusions, and then votes on those conclusions to verify that the majority are in consensus.[3]

Several clear differences exist between DLT and traditional database technology as they were designed to support fundamentally different hypotheses of access to and control of assets. First, in traditional information technology (IT) architectures, each organization manages and secures its own data; blockchain and DLTs represent a departure from this approach. Under this new model, a subset of an organization's total data set becomes a shared asset among network participants, continuously synchronized, and managed via consensus protocols and business rules encoded within the blockchain. Confidentiality, privacy, integrity, and contractual rights are enabled through strong cryptographic techniques including hash codes, and public and private keys.[3,8] A distributed ledger necessitates processes including maintenance and validation, which are performed by a network of communicating nodes.[9] These nodes operate software which synchronizes the copies of the distributed ledger among a peer-to-peer network of participants, making all transactions auditable and sequentially traceable via cryptographically-generated digital fingerprints, or hash codes. Data recorded in this type of ledger are

categorized as pervasive and persistent; it creates a transparent, nearly-immutable record.

Blockchain Vulnerabilities and Strengths

Blockchains are also intrinsically longitudinal data structures, enabling the verification of transactions, as well as capturing the specific sequence of transaction execution within the distributed ledger [8]. Yet contrary to a widely propagated hypothesis asserting that entries in blockchain are immutable, (i.e., they can be altered only by appending a change to a record, but not by deleting or modifying the original record) it is unlikely that any technology is absolutely secure. For example, the integrity of blocks and the data they contain may be vulnerable while being evaluated by the participating nodes; or in the event there is a new consensus protocol for evaluating blocks. This is referred to as a 'consensus fork', a technology event analogous, in principle, to a software update.

Therefore, blockchain technology is more correctly characterized as offering strong resistance against tampering. This pragmatist perspective is based upon IT theory and operations, emerging reports on blockchain data vulnerability, Quantum Resistant Cryptography, vulnerabilities inherent in consensus-based proof-of-work (e.g., mining) model, and other threats to integrity.[10-15]

As all industries are increasingly subject to criminal hacking and related attacks resulting in compromised networks and data, it is imperative that blockchain and DLTs be evaluated in the context of cybersecurity. Traditional database technology typically has security features, including the use of encryption technology, intended to protect the entirety of the data store (i.e., all records, all data elements). Therefore, if those security features are breached, the entirety of the data becomes accessible. By contrast, distributed ledgers can separately encrypt each discreet transaction stored on the blockchain, which represents a superior differentiating characteristic in regard to security.

Distributed Storage

In combination with the append-only, linear, sequential characteristic of blockchain technology, all parties with full nodes have full copies of the blockchain resulting in deliberate redundancy of data. Although this redundancy serves a purpose (e.g., transparency, resilience, verifiability) it also comes with financial costs (e.g., capital equipment, energy consumption, other operating cost, etc.), and compliance risks (e.g., meeting legal and regulatory requirements, government issued advisories, policies, procedures governing institutional participants, etc.).

Multiple factors drive what data are stored on a blockchain. Essentially an optimization-class consideration, the answer depends largely on: (1) what problem(s) the blockchain-enabled solution is designed to solve; (2) which use-cases are in scope of this solution, and; (3) what is the minimally required scope of data to be collected and processed throughout these use-cases (i.e., Data Minimization Principle). Limiting the scope of data stored on a blockchain serves to comply with data protection directives such as the European Union's (EU) General Data Protection Regulation (GDPR), as well as achieving desired performance of the system.

Based on the append-only feature of blockchain, it is nearly impossible to alter previous blocks in the blockchain undetected. This may be at odds with certain rights of people whose data are processed, such as the right to correction if data are recorded inaccurately and the right to be

forgotten. Therefore, special attention should be paid to rights of data subjects, when applying blockchain technology.

Privacy and Blockchains

From a privacy perspective, whether the blockchain is accessible to the general public or only accessible to parties that are privy to a specific blockchain network is significant, including in the context of compliance with the principle of data minimization. Blockchain technology enables granular and traceable permissions unique to each party participating in a given blockchain network. Controlled access can be achieved via encryption to view or process specific data elements within certain time windows and under predetermined circumstances.

In non-permissioned blockchain applications, all participants in that specific blockchain network are free to add data. By contrast, in permissioned blockchain applications, parties are able to add data to the blockchain only in accordance with their unique set of privileges encoded within that application. Because a trusted intermediary is needed to assign and encode such privileges, the allocation of control over the system is not evenly distributed among the network participants. Therefore, the party that is determining the functions and objectives of the application must make design decisions constrained by specific privacy rules, elevating the significance of the choice between permissioned and non-permissioned approaches.

Blockchain and Cryptocurrency

Using blockchain as the underlying technology has given rise to a new type of currency, or system of value tokens that can be managed on the blockchain.[16] Today, this concept is referred to as cryptocurrency. Cryptocurrency is encrypted code used to signify a value of transfer. Alternate coins (altcoins) and tokens are also derived from cryptocurrency. Although regarded as cryptocurrency, the difference between an alt coin and a token depends on the origin. Alt coins are units of value and modes of exchange that originate from its parent blockchain. A token, or tokenization, represents a digital item or asset that is built on top of another such digital item (e.g., ERC-20 token on top of Ethereum, an ether-powered smart contracts blockchain platform.) Tokens generally represent any type of asset class that is traded.

Another way to think about the diverse types of currency blockchain supports is as follows is shown in Table 1.

When considering industry uses for tokens, the value proposition relies on the type of transaction that needs to occur. Any medium of exchange including medical records, healthcare data, and information can be facilitated using tokens. Alternately, cryptocurrencies can be a medium of exchange to support large financial transactions. While the best use case of blockchain is based on the cryptocurrency Bitcoin, the use of blockchain technology does not necessarily imply or require involvement of cryptocurrencies. Blockchains may be used to enable collaboration and secure data exchange across networks, and thereby deliver value to without the use of cryptocurrencies.

Blockchain Consensus Protocols

Blockchain networks are heavily influenced by their consensus algorithms and the associated network protocols. These algorithms and protocols are used by the blockchain nodes in the network to coordinate collaboration to ensure the validity and consistency of decentralized ledgers.

Table 1. Types of currency blockchain supports

Currency	Description
Coins or cryptocurrencies	• General purpose units of digital funds that can be used as a means of payment, investment, or exchange with other coins or cryptocurrencies
Utility tokens	• Special purpose units of digital funds that are intended to be used in exchange for pre-defined goods or services. • Nevertheless, certain utility tokens may be exchanged with other types of cryptocurrencies via cryptocurrency exchange services
Tokenized securities	• Special purpose units of digital funds that are tied to tradeable assets

The particular consensus algorithm in a given blockchain network is a function of the specific blockchain technology used to implement the blockchain network. The performance, throughput, and scalability of blockchain networks are generally network bound, depending heavily on the consensus algorithm and associated network protocol, as well as the latency and bandwidth of the network connecting the blockchain nodes.

Consensus algorithms are typically more conservative and lower performance in untrusted public blockchain networks (e.g., Bitcoin). While in trusted private/consortium blockchains they assume organizations connecting to the network are well-known and trusted, and therefore streamline the consensus algorithm and associated network protocols to improve performance.

BLOCKCHAIN ADOPTION—FROM FINTECH TO HEALTHCARE

Financial Technology

Financial technology (FinTech) is broadly defined as any technological innovation in financial services and was the first conventional sector to explore and adopt blockchain technology. Those engaged in the FinTech industry develop new technologies to disrupt traditional financial markets.[17,18] While Bitcoin, crypto-currencies, and blockchain technology have evolved in parallel with FinTech innovations, blockchain is instrumental in over a dozen FinTech disruptive technologies.[19] Blockchains facilitate peer-to-peer, global value exchange in near real time, using mechanisms that are cryptographically secured.[20] This creates a large-scale method of processing for value exchange in financial.

Healthcare

Healthcare is a system comprised of numerous components, foremost being patients, and including facilities to provide care, suppliers of medicines or equipment, the healthcare workforce to deliver services, educational and research institutions to train the workforce, and payers and government financing mechanisms. Yet to better understand the relevance of blockchain, we propose to expand the definition of the healthcare industry beyond traditional delineation. In this we mean the convergence with life sciences, consumerism, precision medicine, and emerging technologies.[21-26]

The healthcare system in the United States (U.S.) is more decentralized and private than that of other countries.[27] It is in this ecosystem that all the components of healthcare generate information and knowledge to improve health services, healthcare operations and cost, and patient outcomes.

Most data in the healthcare industry today exist in silos within enterprise applications deployed within individual healthcare organizations. Yet

blockchain technology does not cause decades-old problems of interoperability across healthcare data silos to magically go away. Rather, blockchain creates net new, albeit solvable interoperability problems. Examples include on-chain and off-chain use-cases, smart contracts across two or more blockchain platforms, consensus protocols, utility token and coin value exchange, and more.

There is great latent potential to share healthcare data across networks of healthcare organizations to both improve the quality of patient care and reduce costs. The healthcare industry already has multiple types of networks of healthcare organizations from clearinghouse networks, to drug supply chains, provider credentialing networks, health information exchanges, and more.

These existing networks represent near term opportunities for blockchain. In these networks blockchain will likely augment existing enterprise systems and enable secure data sharing to improve patient care and reduce costs. Once blockchain proves its value to healthcare in the near term, this will pave the way for radical new healthcare use cases, types of networks, and values to enable further major improvements in healthcare longer term.[3-6,18,21-24,28-33]

CONSIDERATIONS IN BLOCKCHAIN MODELS FOR HEALTHCARE

An infinite number of variations is possible when applying blockchain technology to the healthcare industry. To help identify the most compelling use cases in healthcare, the following common characteristics in the application of blockchain technology are of notable importance.

Health Data Storage

With blockchain, all sorts of data can be stored, or referenced, such as data specific to conditions, lab results, medications, allergies, and myriad other clinical attributes. Healthcare data also include operational and administrative data (e.g., attributed primary care providers, insurance coverage eligibility, copays, premiums, out of pocket limits, and spending account transactions). It is significant whether data relate to persons or only to organizations from a privacy perspective. Data that can identify, locate, or be used to contact a person represents personally identifiable information (PII). Where personal data and PII are concerned, the privacy rules are applicable. If more sensitive data are also processed (e.g., health data or citizen service numbers) more stringent requirements apply. Health data combined with PII are commonly referred to as protected health information (PHI) and is strictly regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and data protection laws abroad, which can vary by location.

Conceivably, a blockchain-enabled solution would provide innovative design opportunities to harden PII and PHI protection tied to smart contracts, data provenance, optimizing on-chain and off-chain data storage, and data minimization; coupled with individual's governance over others access to and use of their data—in addition, of course, to the data and metadata encryption inherent in blockchain.

Security in the Healthcare Blockchain

A patient's healthcare information must represent trusted, authoritative evidence of care provided, decisions made, treatments and medications prescribed, and identities of participants in the care cycle.[21] Blockchain provides the assurance that data were not tampered with and confirms details of the provenance of the data. Through cryptographic

techniques, such as public and private key pairs and the distributed nature of the blockchain system itself, all information shared has an auditable trail—a traceable, reliable digital "fingerprint".

Confidentiality

To ensure privacy and protect confidentiality of sensitive information, it is necessary to structure to only allow that authorized parties are granted access to sensitive information stored on the blockchain. Confidentiality should not be taken for granted with blockchain and depends on several key design and implementation decisions.

What sensitive patient information goes on the blockchain versus what remains off the blockchain is a key decision that influences the magnitude of the risk to confidentiality. Data minimization is a key principle in privacy and preserving confidentiality. Hence, a minimal, sufficient approach is recommended for decisions on what to include on the blockchain.

Given a specific use case and the set of data fields required on the blockchain to serve it, we support the notion of storing those data elements on the blockchain but leave the remaining data off the blockchain. The decision to store all available sensitive data on the blockchain and later figure out how to use it is discouraged. Nevertheless, zero-knowledge proof whereby a participant in the network can confirm the validity of PII or PHI without exposing the PII or PHI data itself may create opportunities to accelerate time to market of innovative, early-adopter class blockchain solutions in healthcare.

Whether a blockchain is private, permissioned, or public is another key design decision that affects privacy. Scope of access to the blockchain should be limited to authorized entities. If a blockchain truly holds only non-sensitive information intended for public use, then a public blockchain is a reasonable approach. However, in most healthcare blockchains, sensitive information will be stored on the blockchain and only authorized entities should be given access to this information, making private and permissioned blockchains more appropriate. The principle of least privilege is well established in cybersecurity and, applied to private blockchains, requires that entities transacting on the blockchain have minimal but sufficient permissions to fulfill their role on the blockchain network. Sensitive information stored on the blockchain may also be encrypted as a method to further restrict access to only authorized entities and help protect confidentiality and ensure privacy.[34]

Data Integrity vs. the Right to be Forgotten

Protecting the integrity of blockchain data involves protecting against unauthorized deletion or altering of data on the blockchain.

However, this can present different challenges. For example, in a case where a patient has the right to be forgotten, requiring the deletion of their stored PII from the blockchain clashes with the immutability goal of the blockchain-enabled solution. In these cases, PII can be stored off chain and referenced using an opaque unique identifier for the patient on the blockchain; and if a patient exercises their right to be forgotten, their PII off chain can be deleted, effectively de-identifying and anonymizing any associated data on the blockchain.

Availability

Healthcare is inherently a time-sensitive undertaking, hence timely access to data is largely mission-critical. As the industry is anticipated to accelerate experimentation with

and adoption of blockchain-enabled solutions, such ought to meet this requirement.

Yet blockchain's decentralized ledgers provide no single point of failure.[3] Moreover, as we have discussed in the preceding sections of this article, that some of the data will be stored on-chain and the rest will reside off-chain is a core design assumption. Therefore, standard best practices such as redundant blockchain nodes, availability of off-chain systems, load balancing, automatic failover, and redundant network connectivity ought to be implemented to assure high availability.

Furthermore, the design of blockchain-enabled solutions in healthcare ought to consider the tolerance for latency and success/failure rate of adding blocks to the chain (e.g., if a block fails

validation, it will not be added to the chain). Performance optimization techniques may include transaction prioritization, queueing and hatching (i.e., including two or more transactions in a single block); and proper detection, correction, and retry logic strategies and means should be part of the solution design phase.

As we do not envision a single blockchain design pattern for healthcare's high availability challenges, such considerations should be addressed on a use-case by use-case basis.

Adequacy

Healthcare is unfortunately very familiar with breaches involving business associates or data processors. Maintaining the quality and reducing the cost of patient care requires mitigating these risks. This involves a variety of safeguards, including business associate agreements, as well as ensuring the adequacy of security and privacy controls used by the business associates. Blockchain is a new type of middleware that can enable completely new levels of business to business (B2B) networks of healthcare organizations to collaborate. These networks can include both covered entities and business associates.

Potential breaches involving healthcare blockchains could not only impact the quality and cost of patient care but may also impede growth of blockchain in healthcare and the realization of the associated benefits. Effective risk mitigation of these types of breaches requires the following considerations:

1. On-chain or off-chain data breach in a single node of a single healthcare organization would impact the entire blockchain-enabled environment (i.e., all nodes on-chain and off-chain data of all participating organizations);
2. Security risk assessment, capability gap assessment, and security benchmarking should be performed to detect vulnerabilities of all participating organizations – leading to proactive remediation.
3. Holistic security of the blockchain itself, all the nodes running the decentralized ledgers, and all the non-blockchain systems of healthcare organizations that connect to the solution. It entails administrative, physical, and technical safeguards, as well as a multi-layered, defense-in-depth approach at each level.

In so doing, the blockchain-enabled healthcare ecosystem participants would establish, share, and maintain the trust that is key to achieve desired return on adoption of this technology.[34,35]

Compliance

Key factors that determine the scope of compliance requirements for healthcare blockchains include what sensitive data are stored on the blockchain, what are the data usage agreements, and what is the physical location of the blockchain nodes and decentralized ledgers storing this information. For example, where a blockchain stores PHI of U.S. citizens, rules outlined in HIPAA are relevant. Where blockchains store sensitive patient information of European Union (EU) citizens, regulations in General Data Protection Regulation (GDPR) are relevant.

If blockchains span countries or regions with different regulations and data protection laws, such that blockchain nodes, decentralized ledgers, and copies of sensitive data contained within are physically located across these regulatory zones, then trans-border data flow will occur as new sensitive data are added to the blockchains.

In designing blockchains for healthcare, it is very important to understand upfront what compliance requirements are applicable. These can be predicated on data type and sensitivity intended for storage on the blockchain, the deployment architecture of the blockchain network, and where blockchain nodes are physically located.[36] It is also important that blockchain networks may start within a single regulatory zone with no trans-border data flow but may grow later to become international and implicitly add trans-border data flow. Compliance requirements during design of such blockchains should anticipate if such growth could occur and design accordingly.

As discussed previously, requirements such as a patient's right to opt-out of sharing data and the right to be forgotten can have direct impact on what sensitive data can go on the blockchain and what sensitive data must remain off the blockchain. Designing blockchain-enabled solutions that connect healthcare ecosystem participants across multiple geo-political and geo-governance boundaries may explore the use of off-chain encrypted decentralized storage (such as InterPlanetary File System, 'IPFS'), and storage zones for meeting compliance across GDPR, HIPAA, and other.

DEVELOPMENT OF BLOCKCHAIN WITH OTHER TECHNOLOGIES

Interoperability

Interoperability should not be taken for granted with blockchain. It depends on how information is stored on the blockchain, as well as any off-chain data sources referenced subject, of course, to data ownership and access policy. To achieve the trusted interoperability that would match blockchain's data integrity premise, the structure, semantic integrity, reference terminologies and code sets employed, and status of data stored on the blockchain should be defined and enforced.[37-41]

In cases where a blockchain contains pointers to off chain data, metadata associated with such pointers can include information required to support interoperability. This approach enables interoperability not just for the data stored on the blockchain, but also for the data stored off the blockchain. In the former case, interoperability is enforced at the time of adding data to the blockchain, while in the latter case interoperability is required at the time one healthcare organization directly (peer-to-peer) requests a record from another organization in the same blockchain network, based on discovery of the record using metadata stored on the blockchain.

Extending vertical service-level healthcare interoperability application programming

interface (API) patterns (e.g., Fast Healthcare Interoperability Resources; 'FHIR') to call and serve data transactions via emerging blockchain APIs (e.g., DApps) and smart contracts may lead to on-chain/off-chain solutions that optimize the industry's need for mission critical availability and security.

Deployment Architecture

Blockchains may be deployed either on public platforms such as Ethereum, or in private blockchains with nodes either in perimeter networks of participating healthcare organizations or in cloud environments. Each option has major implications to privacy, security, compliance, performance, deployment, and ongoing operational and maintenance costs. Careful proactive consideration should be given up front to the blockchain deployment option and its ramifications.

CONCLUSIONS

Blockchain is a disruptive technology. As such, it challenges legacy thinking about business and operational models of the expanded healthcare universe without borders, data ownership, and data use—while offering new opportunities not previously deemed feasible nor practical.

Blockchain is also currently surrounded by hype and presented as a panacea for various challenges. It is attracting tremendous attention and resources—from entrepreneurs to investors, economic buyers, policy makers, and consumers around the world. The encrypted distributed ledger has potential to improve the quality of patient care, as well as the economics and efficiency of healthcare operations, particularly considering growing data volumes with emerging data sources such as Internet of Things (IoT). Other blockchain characteristics, notably near-immutability, smart contracts, and off-chain interoperability open up opportunities to tie in applications and services that extend beyond legacy boundaries of healthcare.

Going forward, we call for rapidly and broadly disseminating 'low-hanging-fruit' use-cases such as supply chain, medication ePedigree, medical device identity and certification, and claims management. Rapid prototyping of 'how it works for the user' (i.e., User Experience; 'UX'), Proof-of-Concept pilots, and sharing of key learnings from early adopters are needed to keep the innovation and discovery momentum going. Constructing and evaluating blockchain solutions roadmaps and value proof points would help patients, healthcare consumers, and ecosystem players around the world reach the ultimate goal: return on adoption.

Acknowledgement

Invaluable contributions for the development of this manuscript ranging from ideation to critical review were provided by fellow members of the Health Information and Management Systems Society (HIMSS) Blockchain Working Group. The authors would also like to thank Katie Crenshaw and Mari Greenberger for providing the impetus and logistical support for creation of this work.

Funding Statement

There was no public or private funding provided in the creation of this work.

Conflict of Interest

The authors whose names are listed immediately below report the following details of affiliation or involvement in an organization or entity with a financial or non-financial interest in the subject matter or materials discussed in this manuscript.

RR: Founder and CEO of R&D Ribitzky, a specialty consulting firm serving the healthcare

information technology, life sciences informatics, and Precision Medicine ecosystem worldwide, has financial and other interest in pre-existing and future projects pertaining to the subject matter and materials discussed in this manuscript; serves on the Advisory Board of ARNA Genomics and BitMed.

JS: Founder, The Institute for Healthcare Financial Technology (HealthFinTech) is a non-profit organization dedicated to improving the healthcare value chain to reduce costs and streamline access and delivery of healthcare. HealthFinTech builds on the innovations of financial technology ("fintech") and healthcare technology, especially such concepts as Artificial Intelligence (AI), blockchain and distributed ledgers.

CTM: Founder and CEO of Patientory.

BA: Employed by Medicity, an Aetna business. No other disclosures

HLF: Founder and majority owner of Obesity PPM, a disease management and population health company founded in 2009 with emerging blockchain-specific service offerings.

KAC: Has served as a consultant for blockchain companies focused on healthcare and healthcare companies exploring blockchain solutions.

The authors whose names are listed immediately below certify that they have NO affiliations with or involvement in any organization or entity with any financial interest (such as honoraria; educational grants; participation in speakers' bureaus; membership, employment, consultancies, stock ownership, or other equity interest; and expert testimony or patent-licensing arrangements), or non-financial interest (such as personal or professional relationships, affiliations, knowledge or beliefs) in the subject matter or materials discussed in this manuscript.

DIH: No conflict of interest to disclose.

MG: No conflict of interest to disclose.

EP: No conflict of interest to disclose.

Contributors

To fulfil all of the criteria for authorship, every author of the manuscript has made substantial contributions to **ALL** of the work and participated sufficiently in the work to take public responsibility.

References

1. Regenscheid A. Blockchain and distributed ledger technologies: opportunities, challenges and future work [Internet]. Washington (DC): National Institute of Standards and Technology; 2017 Jun 28 [cited 2017 Dec 29]. Available from: https://csrc.nist.gov/CSRC/media/Presentations/NIST-Block-Chain-Research-Project/images-media/ar-dy-blockchain-combined.pdf

2. Peck ME. Blockchains: how they work and why they'll change the world. *IEEE Spectrum*; 2017 Sep 28 [cited 2017 Dec 29]. Available from:

https://spectrum.ieee.org/computing/networks/blockchains-how-they-work-and-why-theyll-change-the-world

3. Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications [Internet]. *J Am Med Inform Assoc*. 2017 Nov 1 [cited 2017 Dec 29];24(6):1211-1220. Available from: https://www.ncbi.nlm.nih.gov/pubmed/29016974 doi: 10.1093/jamia/ocx068

4. Halamka JD, Lippman A, Ekblaw A. The potential for blockchain to transform electronic health records [Internet]. Cambridge (MA): *Harvard Business Review*; 2017 Mar 3 [cited 2017 Dec 29]. Available from: https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records

5. Capital Consulting Corporation's Innovation Center. Use of blockchain in health IT and health-related research challenge [Internet] Capital Consulting Corporation; 2016 [updated 2016 Jul 7, cited 2017 Dec 29]. Available from: https://www.cccinnovationcenter.com/challenges/block-chain-challenge/

6. Cookson R. NHS urged to adopt bitcoin database technology [Internet]. *Financial Times*; 2016 Jan 19 [cited 2017 Dec 29]. Available from: https://www.ft.com/content/c4bad1ec-bea3-11e5-846f-79b0e3d20eaf

7. Suberg W. Alibaba deploys blockchain to secure health data in Chinese first. *Cointelegraph*; 2017 Aug 18. [cited 2017 Dec 29]. Available from: https://cointelegraph.com/news/alibaba-deploys-blockchain-to-secure-health-data-in-chinese-first

8. Brodersen C, Kalis B, Mitchell E, Pupo E, Triscott A. Blockchain: securing a new health interoperability experience. [Internet] Accenture LLP; 2016 Aug 8. [cited 2017 Dec 29]. Available from: https://www.healthit.gov/sites/default/files/2-49-accenture_onc_blockchain_challenge_response_august8_final.pdf

9. Borne FL, Treat D, Dimidschstein F, Brodersen C. SWIFT on distributed ledger technologies. Delivering an industry-standard platform through community collaboration. [Internet] SWIFT SCRL 2016; [cited 2017 Dec 29]. Available from: http://www.ameda.org.eg/files/SWIFT_DLTs_position_paper_FINAL1804.pdf

10. Sharma N. Is quantum computing an existential threat to blockchain technology? [Internet]. SingularityHub. Singularity Education Group; 2017 Nov 5. [cited 2017 Dec 29]. Available from: https://singularityhub.com/2017/11/05/is-quantum-computing-an-existential-threat-to-blockchain-technology/#sm.0001uwpacl916evdywh11fcvhcht6

11. Castor A. Why quantum computing's threat to bitcoin and blockchain is a long way off [Internet]. *Forbes*; 2017 Aug 25 [cited 2017 Dec 29]. Available from: https://www.forbes.com/sites/amycastor/2017/08/25/why-quantum-computings-threat-to-bitcoin-and-blockchain-is-a-long-way-off/#81458a228829

12. Rodenburg B, Pappas SP. Blockchain and quantum computing [Internet]. Princeton (NJ): *Mitre*; 2017 Jun. 16 p. [cited 2017 Dec 29]. Available from: https://www.mitre.org/sites/default/files/publications/17-4039-blockchain-and-quantum-computing.pdf

13. Aggarwal D, Brennen GK, Lee T, Santha M, Tomamichel M. Quantum attacks on Bitcoin, and how to protect against them [Internet]. New York (NY): Cornell University Library arXiv.org; 2017 Oct 28 [cited 2017 Dec 29]. Available from https://arxiv.org/pdf/1710.10377v1.pdf arXiv:1710.10377v1

14. Conti M, Kumar S, Lal C, Ruj S. Survey on security and privacy issues of bitcoin [Internet]. New York (NY): Cornell University Library arXiv.org; 2017 Dec 25. [cited 2017 Dec 29]. Available from: https://arxiv.org/pdf/1706.00916.pdf arXiv:1706.00916v3

15. Eyal I. The miner's dilemma. 2015 IEEE Symposium on Security and Privacy. IEEE; 2015:89–103.

16. El Bahrawy A, Alessandretti L, Kandler A, Pastor-Satorras R, Baronchelli A. Evolutionary dynamics of the cryptocurrency market. *R Soc Open Sci* [Internet]. 2017 Nov 15 [cited 2017 Dec 29];4(11):170623. Available from: http://rsos.royalsocietypublishing.org/content/4/11/170623 doi: 10.1098/rsos.170623

17. Browne R. Everything you've always wanted to know about fintech [Internet]. CNBC; 2017 Oct 4. [cited 2017 Dec 29]. Available from: https://www.cnbc.com/2017/10/02/fintech-everything-youve-always-wanted-to-know-about-financial-technology.html

18. Till BM, Peters AW, Afshar S, Meara J. From blockchain technology to global health equity: can cryptocurrencies finance universal health coverage? *BMJ Glob Health.* 2017 Nov 10;2(4):e000570. Available from: https://www.ncbi.nlm.nih.gov/pubmed/29177101 doi: 10.1136/bmjgh-2017-000570

19. CB Insights. The FINTECH 250 [Internet]. CB Insights; 2017 [cited 2017 Dec 29]. Available from: https://www.cbinsights.com/research-fintech250

20. Skinner C. Blockchain is fintech's real game-changer. Source Media; 2016 Mar 21. [cited 2017 Dec 29]. Available from: https://www.americanbanker.com/opinion/blockchain-is-fintechs-real-game-changer

21. Halamka JD. Life as a Healthcare CIO. The blockchain challenge [Internet]. 2016 Aug 31 [cited 2017 Dec 29]. Available from: http://geekdoctor.blogspot.com/2016/08/the-blockchain-challenge.html

22. Ekblaw A, Azaria A, Halamka JD, Lippman A. A Case Study for Blockchain in Healthcare: "medrec" prototype for electronic health records and medical research data [Internet]. IEEE; 2016 Aug. [cited 2017 Dec 29]. Available from: http://dci.mit.edu/assets/papers/eckblaw.pdf

23. Shrier AA, Chang A, Diakun-thibalt N, Forni L, Landa F, Mayo J, et al. Blockchain and health it: algorithms, privacy, and data. Washington (DC): Office of the National Coordinator; 2016 Aug 8. [cited 2017 Dec

29]. Available from: https://www.healthit.gov/sites/default/files/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf

24. Gordon W, Wright A, Landman A. *N Engl J Med Catalyst*. Blockchain in health care: decoding the hype [Internet]. (MA): Massachusetts Medical Society; 2017 Feb 9 [cited 2017 Dec 29]. Available from: https://catalyst.nejm.org/decoding-blockchain-technology-health/

25. Ribitzky R. The precision medicine paradox [Internet]. LinkedIn; 2017 Jun 19 [cited 2017 Dec 29]. Available from: https://www.linkedin.com/pulse/precision-medicine-paradox-ron-ribitzky-m-d-/

26. Ribitzky R, Karnieli E, Rishe N, Yesha Y, Liebschutz A. Knowledge mining and bioinformatics techniques to advance personalized diagnostics and therapeutics – the case for white space R&D [Internet]. Report to the National Science Foundation NSF Industry-University Cooperative Research Center for Advanced Knowledge Enablement; 2014 Jun 22 [cited 2017 Dec 29]. Available from: http://hit.fiu.edu/NSF-Report/NSF_Post-Workshop_Book_White_Space_RD_Knowledge_Mining_Personalized_Medicine.pdf

27. Goldsteen, RL, Goldsteen, K, Goldsteen, BZ. Jonas' introduction to the U.S. health care system. 8th ed. New York (NY): Springer Publishing; 2017

28. Peters AW, Till BT, Meara JG, Afshar S. Blockchain technology in health care: a primer for surgeons [Internet]. 2017 Dec 6 [cited 2017 Dec 29];102(12). Available from: http://bulletin.facs.org/2017/12/blockchain-technology-in-health-care-a-primer-for-surgeons/#.Wkv3U1WnEUF

29. Marr B. This is why blockchains will transform healthcare. *Forbes*; 2017 Nov 29 [cited 2017 Dec 29]. Available from: https://www.forbes.com/sites/bernardmarr/2017/11/29/this-is-why-blockchains-will-transform-healthcare/#4e37cc71ebe3

30. Versel N. Blockchain eyed for boosting data security, trust in precision medicine. GenomeWeb LLC; 2017 Aug 23. [cited 2017 Dec 29]. Available from: https://www.genomeweb.com/informatics/blockchain-eyed-boosting-data-security-trust-precision-medicine

31. Versel N. Despite hype, blockchain remains mostly theoretical in precision medicine. GenomeWeb LLC; 2017 Aug 31. [cited 2017 Dec 29]. Available from: https://www.genomeweb.com/informatics/despite-hype-blockchain-remains-mostly-theoretical-precision-medicine

32. Ichikawa D, Kashiyama M, Ueno T. Tamper-resistant mobile health using blockchain technology. *JMIR Mhealth Uhealth*. 2017 Jul 26 [cited 2017 Dec 29];5(7):e111. Available from: https://www.ncbi.nlm.nih.gov/pubmed/28747296 doi: 10.2196/mhealth.7938

33. Wilde V. Could blockchain technology help? re: the hackers holding hospitals to ransom. *BMJ* [Internet] 2017 May 10 [cited 2017 Dec 29];357:j2214. Available from: http://www.bmj.com/content/357/bmj.j2214/rr-6 doi: https://doi.org/10.1136/bmj.j2214

34. Houlding D. Intel. Healthcare blockchain: what goes on chain stays on chain [Internet]. Intel Corporation; 2017 Aug 23 [cited 2017 Dec 29]. Available from: https://itpeernetwork.intel.com/healthcare-blockchain-goes-chain-stays-chain/

35. Chang V. Delivery and Adoption of Cloud Computing Services in Contemporary Organizations. Hershey: IGI Global; 2015

36. Alferes JJ, Bertossi L, Governatori G, Fodor P, Roman D. Rule technologies. research, tools, and applications. Stony Brook (NY): 10th International Symposium, Rule ML; 2016, Jul 6-9, 2016. [cited 2017 Dec 29]. Available from: https://link.springer.com/book/10.1007/978-3-319-42019-6?no-access=true

37. Houlding D. Intel. Healthcare blockchain: does your chain have any weak links? Intel Corporation; 2017 Nov 14 [cited 2017 Dec 29]. Available from: https://itpeernetwork.intel.com/healthcare-blockchain-chain-weak-links/

38. Houlding D. LinkedIn. Will blockchains deliver healthcare interoperability? 2017 Dec 21 [cited 2017 Dec 29]. Available from: https://www.linkedin.com/pulse/blockchains-deliver-healthcare-interoperability-houlding-cissp-cipp/

39. Health Information and Management Systems Society (HIMSS). The interoperability imperative: value-based care depends on health information exchange [Internet]. Chicago (IL): Healthcare Information and Management Systems Society (HIMSS); 2017 Feb [cited 2017 Dec 29]. Available from: http://www.healthcareitnews.com/himss-infocus/interoperability?aliId=851543264

40. Runyon B. An overview of healthcare interoperability and key considerations for upcoming challenges [Internet]. Stamford (CT): Gartner; 2017, Feb 15. [cited 2017 Dec 29]. Available from: https://www.gartner.com/doc/3610117?ref=AnalystProfile&srcId=1-4554397745

41. Modern Healthcare. Chief information officers roundtable: the challenges are getting tougher. Modern Healthcare; 2017 Apr 1 [cited 2017 Dec 29]. Available from: http://www.modernhealthcare.com/article/20170401/magazine/304019951