Journal of Digital Imaging (2020) 33:726–734
https://doi.org/10.1007/s10278-019-00310-3

Blockchain Technology: Principles and Applications in Medical Imaging

Morgan P. McBee[1] · Chad Wilcox[2]

Published online: 2 January 2020

Abstract
Blockchain is an immutable, encrypted, distributed ledger technology. While initially devised for and most commonly referenced with cryptocurrencies, there are an increasing number of applications outside finance, many of which are relevant to medical imaging. In this paper, the concepts and principles underlying the technology and applications relevant to medical imaging are discussed, in addition to potential challenges with implementations such as public versus private key access, distributed ledger size constraints, speed, complexity, and security pitfalls. Potential use cases for blockchain specifically relevant to medical imaging include image sharing including direct patient ownership of images, tracking of implanted medical devices, research, teleradiology, and artificial intelligence. While blockchain offers exciting ways to facilitate the storage and distribution of medical images, similar to the advent of picture archiving and communication systems decades ago, it does have several key limitations of which healthcare providers of medical imaging and imaging informatics professionals should be aware.

Keywords Blockchain · Distributed ledger · Smart contract · Disruptive technology

Introduction

Blockchain is an immutable (i.e., "write once"), distributed, encrypted database technology with a continuously growing list of records (blocks). While a relatively new technology, its uses have expanded exponentially in the financial sector and have even more recently expanded into other fields including medicine. In a recent analysis of startup companies and trends relevant to radiology, blockchain technology was identified as the fastest growing cluster [1]. This article offers a history of blockchain technology, outlines the conceptual framework of its applications, and describes extant and potential applications to medical imaging.

✉ Morgan P. McBee
mcbeem@musc.edu

Chad Wilcox
wilcoxmdma@gmail.com

[1] Department of Radiology, Medical University of South Carolina, 96 Jonathan Lucas Street, Charleston, SC 29425, USA

[2] Department of Radiology, University of California Los Angeles, 757 Westwood Plaza, Los Angeles, CA 90095, USA

History of Blockchain

The foundation for blockchain technology was laid in a 1991 paper which described a system to verify the authenticity of digital documents via hash functions. The authors concluded that it would be possible to accomplish this either through a central authority or by distributing timestamping of hashes [2]. The term "block chain" was first coined in October 2008 in a paper that established the mathematical basis for the Bitcoin cryptocurrency. The cryptocurrency was created in response, or as a reaction to, the 2007 global financial disaster, and the digital currency debuted the year following the paper [3]. The paper was self-published under a pseudonym and has never appeared in a peer-reviewed journal. The true identity of its author still remains unknown.

Since cryptocurrencies are digital and can be easily duplicated, the same money could be sent to two different parties simultaneously, which is known as the double spending problem. Solving the double spending problem was one of the initial driving factors behind the development of blockchain technology [3]. Previously, trust was placed in a central intermediary (such as a bank) which would verify that money has not been sent to more than one party. Blockchain, however, solves the double spending problem by replacing trust in a central intermediary with the concept of cryptographic proof.

Bitcoin was the first cryptocurrency developed which utilizes blockchain technology. It is categorized as a "decentralized virtual currency" by the US Treasury [4]. As of May 2019, Bitcoin has a market cap of over $145 billion USD [5]. Since the advent of Bitcoin, there has been an increasing number of cryptocurrencies introduced.

The introduction of the Bitcoin cryptocurrency in 2009 was the start of blockchain 1.0 technology. Blockchain 2.0 refers to distributed ledgers with smart contracts, which are simply algorithms programmed into the blockchain that allow self-execution of digital transactions based upon predefined criteria. Blockchain 3.0 has been proposed to denote nonfinancial applications of the distributed ledger technology [6] such as use cases in healthcare.

There has been a significant amount of attention given to blockchain technologies by the media. In the Gartner hype cycle, most blockchain technologies remain in the early Innovation Trigger or Peak of Inflated Expectations phases [7] leading many observers to dismiss the technology as a buzzword technology without real world use cases [8, 9]. However, as described in the Applications/Use Cases section in this paper, there are several ways that blockchain can transform and improve medical imaging. The number of use cases is relatively limited, though, and blockchain is far from a panacea for medical imaging or healthcare in general.

Blockchain Principles

The technology underpinning blockchain has several important features. An example of a blockchain implementation is illustrated in Fig. 1. Blockchain is a technological framework and not a specific standard or implementation. As such, there are common principles underlying the various implementations, but not all implementations are the same.

Each block in the chain contains a series of transactions. The simplest way to think about a transaction is in terms of financial transactions or exchanges of money as these were the initial discrete data elements comprising cryptocurrency blockchains such as Bitcoin [3]. However, transactions do not have to be financial in nature and can be any event that results in a change in the blockchain. For example, adding a medical imaging study to a blockchain could be a transaction. In the Ethereum network, applications can be stored within the blockchain, and every transaction results in a change of the distributed application [10]. To expand upon the previous example, machine learning algorithms could be distributed across the Ethereum network, and a transaction could take place whenever a new medical imaging study is added to the blockchain.

Blockchain as a Decentralized Network

Computer networks can be broadly categorized as either centralized or decentralized/distributed (Fig. 2). Centralized networks have a single point of failure. If the central node goes down, the entire network becomes non-functional as all information must flow through this central node. All trust is placed in the central node which is the arbiter of truth. Some hospital intranets and local picture archiving and communication system (PACS) networks are examples of such networks. Decentralized networks do not have a single point of failure but instead have several nodes through which data can be

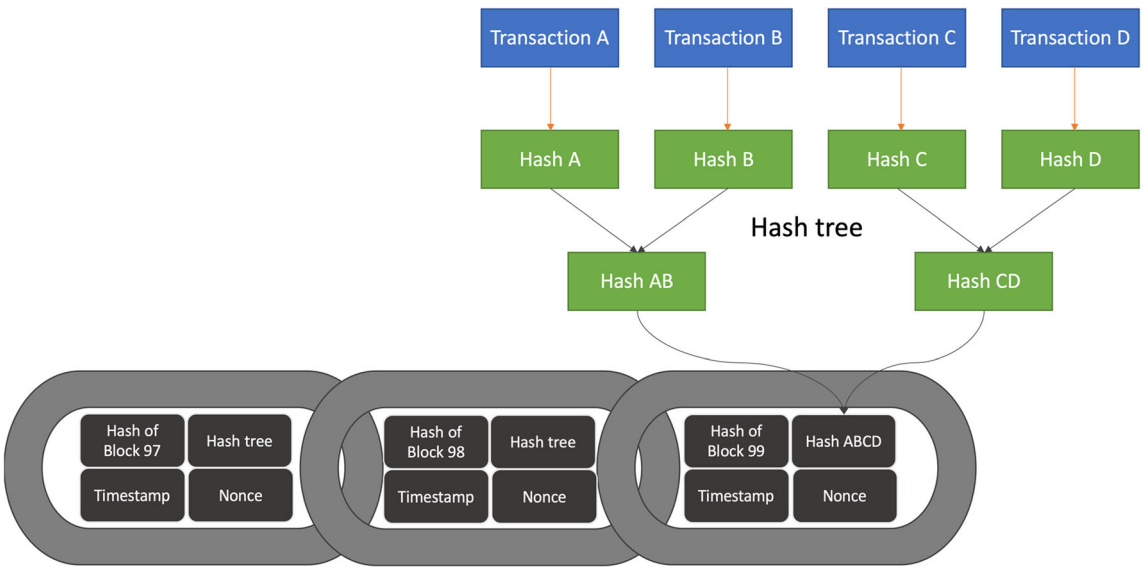

Fig. 1 Blockchain example. Multiple transactions (such as transfers of money) take place. Each transaction is hashed. Hash values are combined into a hash tree. The hash tree, hash of the previous block, and a timestamp are inserted into the new block. Nonces are used in this example as a proof-of-work consensus mechanism as part of a mathematical challenge. When a solution is found to the challenge, the new block is added to the blockchain

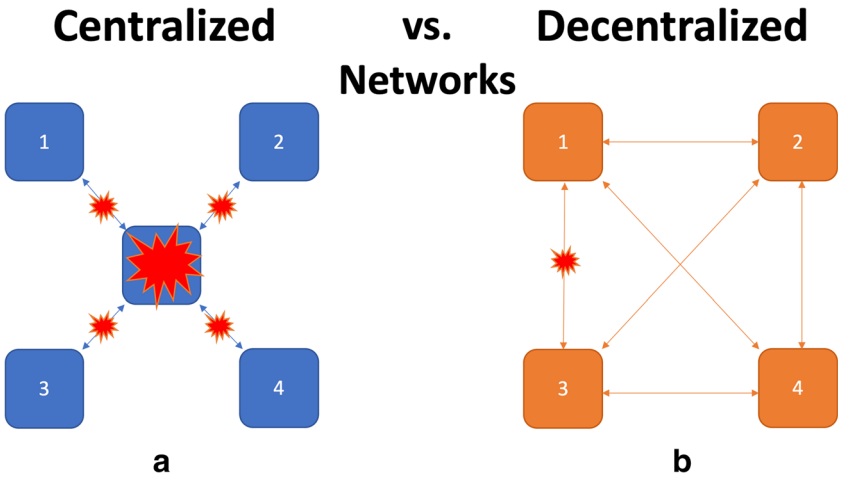

Fig. 2 Centralized vs. decentralized networks. **a** Centralized networks have a single point of failure. If the central node goes down, the entire network becomes nonfunctional. All trust is placed in the central authority which is the arbiter of truth. **b** Decentralized networks do not have a single point of failure. If one or more nodes go down, there is sufficient redundancy that the remainder of the network remains functional. All the nodes must arrive at a consensus as to what the truth is

routed thereby increasing redundancy. If one or more nodes go down, there is sufficient redundancy so that the remainder of the network remains functional. The network topology with the highest redundancy is a decentralized network, as all nodes within the network have the ability to communicate directly with each other [11].

A public blockchain implementation is an example of a decentralized network topology and is composed of individual nodes which can each store an entire copy of the database. Nodes must arrive at a consensus as to which block will next be added to the blockchain. In this manner, blockchain technology enables distributed ledgers and databases. However, decentralization is not an absolute requirement for blockchain implementations as illustrated in the section below on permissioned blockchains.

Consensus

Consensus simply means that all the decentralized nodes in the blockchain network agree upon what constitutes truth. Only the blocks that all nodes agree upon will be appended to the blockchain. The most widely utilized mechanism to achieve consensus in cryptocurrency blockchains is a proof-of-work algorithm [12]. This requires computation of a difficult-to-solve mathematical cryptographic challenge, which is called mining. Once the problem is solved, the other nodes verify the solution with an algorithm that is much more computationally simple than the one required to solve the problem [3].

Proof-of-work authentication depends on the discovery of a "nonce," a unique random or pseudo-random number which, when processed or "hashed" through an algorithm, satisfies arbitrary conditions set by the blockchain (for example, a value beginning with a certain number of zeroes) and enables the data to be added to the blockchain. This task shifts the computational burden of satisfying these conditions to the party seeking to add to the blockchain, and encourages addition of valuable data instead of random data or noise. Changing the arbitrary conditions can make a nonce more difficult (more computational power) or less difficult depending on the desired activity and size of blockchain. The unique nature of the nonce also prevents duplicate additions to the blockchain. The proof-of-work is then recorded on the blockchain and distributed to global blockchain nodes. Each node then undertakes verification of the proof-of-work inclusion, by which process consensus is reached.

Other examples of consensus algorithms include proof of stake, proof of elapsed time, proof of burn, and Byzantine fault tolerance [12]. Technical details of each are beyond the scope of this article, but each has its own unique benefits and drawbacks, and some are more applicable to certain situations and tasks than others.

Immutability

A blockchain is immutable in that data can only be added; blocks can neither be modified nor removed. Once data are appended, they are a permanent part of the blockchain; this is conceptualized as adding "links" to the chain, which grows with each addition. Each block contains a timestamp in addition to a hash value of the previous block's header which links the data in a "chain" of blocks (Fig. 1).

If an attacker were able to modify a block, all the subsequent blocks in the chain would also have to be modified since the hash value of the modified block would change thereby changing the hash values of subsequent blocks since the hash value of the prior block's header is stored within each block. The computational cost of this with current technology is great enough to deter such an attack.

Data Provenance

Provenance is defined as the "the history of ownership of a valued object or work of art or literature" [13]. Data

provenance simply applies this concept to data to enable verification of the source and is made possible by blockchain because each transaction is inherently linked to the previous one. It is a key component of blockchain technology as each block in the chain contains a reference to the previous block, and transactions can be traced all the way back to the genesis block (the first block in a blockchain).

Encryption

Blockchain relies on encryption via public-key cryptography (Fig. 3) which uses key pairs; public keys are publicly available, and private keys are kept secret like passwords. Each actor interacting with the blockchain has a separate public key and private key. As an example, Charlie can send Leah an encrypted message that is only readable by Leah. Using Leah's public key, Charlie can encrypt a message which can only be decrypted with the use of Leah's private key. The data are unreadable without the private key and are thus encrypted.

Hash functions (H) are an important component and map input data (x) to fixed size outputs (h) called hash values (Fig. 4). Cryptographic hash functions are non-invertible (or "one-way") in that an input maps to a given hash value but not vice versa (i.e., the original input cannot be reconstructed from the hash value, but the input data will always produce the same hash value) [2].

Public vs. Private vs. Hybrid Blockchains

As with any blockchain implementation, there are many decisions that must be made about how it will operate. One major decision is whether the blockchain should be permissionless or permissioned. Blockchains may be either public and accessible by everyone or private with only pre-approved participants having access. The difference between the two is akin to the difference between the Internet and a hospital's local intranet [14].

Cryptocurrencies (e.g., Bitcoin and Ethereum) are examples of public blockchain networks in which any computer on the Internet has access to the data stored in the blockchain. Most enterprise applications (e.g., those utilizing Hyperledger Fabric) utilize private blockchains in which permissioning mechanisms control which actors have access to the data stored on the blockchain [10]. However, there exists a continuum between public and private blockchains, known as hybrid, partially decentralized, or consortium blockchains [11].

In order to comply with privacy regulations, such as Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH Act), and in order to maintain utmost security, most enterprise-level applications of blockchain technology within healthcare will likely utilize private/permissioned blockchains. However, as blockchain technology matures and legislation catches up with the technology, storage of protected health information within permissionless blockchains may be a possibility in the future. There have been several permissionless blockchain implementations of electronic medical records (EMRs) made possible by the usage of encryption, which is a necessary first step in any blockchain implementation which makes protected health information available to download by anyone on the Internet.

Distributed Blockchain Ledgers vs. Traditional Databases

Relational databases have been the mainstay of database implementations essentially since their inception in the 1970s. They are quite efficient and scalable. More recently, however, non-relational databases have become more and more popular. Table 1 summarizes the key differences between traditional (relational and non-relational) databases and blockchain.

Traditional databases, in general, allow for modification of data and are therefore not immutable. While immutable implementations of traditional databases are possible, it is

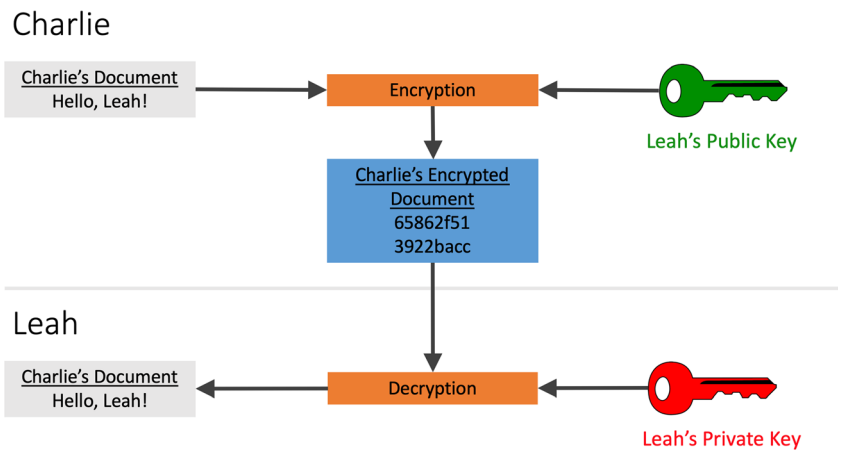

Fig. 3 Public key cryptography. Blockchain relies on public key cryptography which uses key pairs (*public keys* are publicly available, and *private keys* are kept secret like passwords). Using Leah's public key, Charlie can encrypt a message which can only be decrypted by Leah with the use of Leah's private key. The data are encrypted as the message is unreadable without the private key

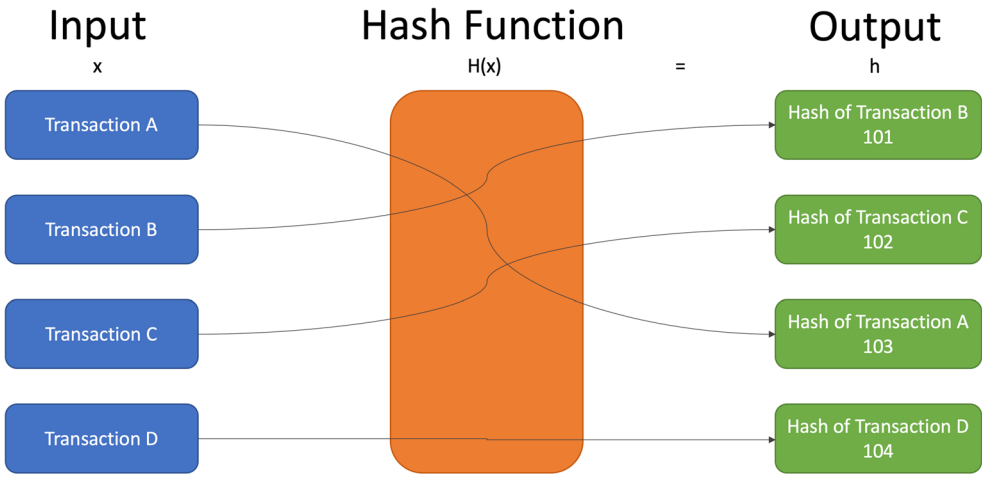

Fig. 4 Hash functions (H) map input data (x) to fixed size outputs (h) called hash values. Cryptographic hash functions are non-invertible in that an input maps to a given hash value but not vice versa (i.e., the input cannot be reconstructed from the hash value)

not a key underlying principle of their technology as it is with blockchain. Traditional databases have the advantage of having low latency allowing for many transactions to be performed concurrently as opposed to blockchain which has high latency and can only support a limited number of transactions at a time. While traditional databases can have redundancy built in, they do not have the advantage of being replicated on every node like blockchain.

Blockchains, in general, are significantly more costly for data storage compared with traditional databases. In fact, the Bitcoin protocol currently limits the size of each block to 1 megabyte [15], but there is a significant debate among the community if this should be increased [16]. As such, most public blockchain implementations are not a viable solution for the storage of large amounts of data such as medical images. To counterbalance this, hashes of the data instead of the raw data can be stored within the blockchain. Specific to medical imaging datasets utilizing the Digital Imaging and Communications in Medicine (DICOM) format, hashes of the pixel data can be stored as the DICOM header may actually change (e.g., when images are transferred to another DICOM device). Conversely, in blockchain frameworks where image data location and access is verified by the blockchain as opposed to stored on the blockchain, this DICOM variability could serve as a robust unique identifier in public/private key transactions, hashed before encryption to ensure the protection of confidential patient information on a public blockchain [17].

Large volume data, as would be expected from thousands of individual images in a multisequence cross-sectional examination, would thus pose a potential obstacle for blockchain storage. However, the concept of "on-blockchain" references to "off-blockchain" images may offer a compromise. While the feasibility of moving a PACS network onto the cloud has been demonstrated [18–21], this solution suffers from the pitfalls of centralization, and scalability to huge image-rich databases in the future may prove problematic. More research must be conducted as to whether image hashes could function as reference values to image data stored on cloud networks.

Completely decentralized storage networks have proven feasible for other applications. Filecoin, for example, is a proprietary decentralized storage network relying on blockchain

Table 1 Blockchain vs. traditional databases. Traditional databases, in general, allow for modification of data and are therefore not immutable. They have the advantage of having low latency allowing for many transactions to be performed concurrently as opposed to blockchain which has high latency and can only support a limited number of transactions at a time. While traditional databases can have redundancy built in, they do not have the advantage of being replicated on every node like blockchain

	Traditional database	Blockchain
Immutable	No	Yes
Operations	Create, read, update, delete	Insert/append only
Number of nodes	Few	Many
Redundancy	Centralized, prone to single point of failure	Can be fully replicated within every node
Consensus	Central authority	Majority of peers agree on outcome of transactions
Latency	Low	High
Transactional Cost	Low	High

principles. Data storage on local, distributed machines is incentivized by issuance of tokens to "miners," and clients pay "miners" upon retrieval of the said data. Similar distributed storage platforms include Sarm, BigChainDB, Interplanetary File System (IPFS), and Storj [18, 19].

Limitations

While blockchain has many potential use cases and benefits, it does have several key limitations.

Complexity

With an ever increasing number of blockchain implementations utilizing different underlying technologies, the ability of different systems to work together will suffer. Additionally, there are bound to be unforeseen complications when smart contracts interact across different blockchain implementations without any human interaction. Much as the DICOM standard enabled interoperability between different vendors and systems, standardization will be necessary as healthcare blockchain implementations move forward.

Privacy/Confidentiality

Public blockchains are at risk of having the stored information exposed if vulnerabilities are 1 day discovered in their underlying encryption schemes. If the encryption is broken, all the data stored in the blockchain could be exposed. While impossible with today's technology, future advances such as quantum computing could enable such a possibility [22]. However, private or permissioned blockchain implementations can mitigate this risk.

Speed/Scalability

Blockchain is considerably slower than traditional databases, and adding new data is limited by the speed of the underlying consensus mechanisms. Traditional database systems are able to scale by adding more servers and therefore more computational power to distribute the workload. With decentralized blockchains, however, every node must participate in consensus. Therefore, more computational power would have to be added to every single node to increase throughput.

With the consensus algorithms most widely employed in the blockchains powering cryptocurrencies (proof-of-work), the mathematical problems that must be solved to create new blocks are becoming increasingly more computationally demanding and thus require a significant amount of electricity [23]. Private blockchains can utilize a much less computationally demanding consensus algorithm but still require more energy than traditional databases. One method to reduce the transaction costs is to only allow certain nodes to participate in consensus [24]; however, some redundancy is lost by doing so.

Security

If a private key were lost, the data would be rendered permanently unreadable. For this reason, further research is warranted to develop novel ways to prevent keys from being lost or forgotten, such as biometric key generation.

Additionally, blockchains are at risk of what is known as a "51% attack." If an attacker were to take control of 51% or more of the nodes comprising the blockchain network, the consensus mechanism could be overridden allowing for double spending.

Given these limitations, it is unlikely that blockchain will completely supplant the traditional database systems currently powering EMRs, picture archiving and communication systems (PACS), and Vendor Neutral Archives (VNAs) but can instead supplement them to extend and enhance their capabilities.

Applications/Use Cases

As cryptocurrency was the original use case for blockchain technology, it is no surprise that it is the most widespread. As transactions stored within blockchains can utilize any kind of metadata and not just transfers of money, an increasing number of use cases utilize the technology for distributed databases or ledgers.

There have been few enterprise-level blockchain implementations in healthcare. However, there are many other use cases in healthcare in which the technology could be beneficial. Biomedical applications of blockchain technology include EMRs, wearables and embedded technology, mobile health, research and clinical trials, medical supply chains, biomedical databases [25], insurance claims [26], credentialing and licensure [27, 28], and public health surveillance [29]. As of this writing, the main focus within the healthcare sector has been on EMRs [17, 25, 30]. Notable large-scale implementations of EMRs built on blockchain technology include MedRec [24], Gem Health Network [25], and Guardtime which has secured over 1 million medical records in Estonia [26]. Text-based healthcare notes and lab values are much more amenable to being distributed on a blockchain as the data size is much smaller than the large datasets common in medical imaging.

Specifically within medical imaging, blockchain use cases include image sharing (including patient-driven/centered ownership of images), teleradiology, research, and machine learning/artificial intelligence applications. It is more practical to store hashes, metadata, or references/links to images within

the blockchain as opposed to images themselves as illustrated in one proposed blockchain implementation for sharing of images [31]. This is especially true because of the slow speed and high cost of storing large amounts of data in a public blockchain. However, entire image datasets could be stored within a private blockchain, or a combination of "on-blockchain" references to "off-blockchain" images could be employed, as discussed above.

Image Sharing

Despite the unanimous adoption of the Internet by healthcare systems and initiatives such as RSNA Image Share [32], medical images are still largely transferred among institutions by compact disc (CD) or digital versatile disc (DVD). Many times, patients themselves are responsible for taking a disc from one healthcare system to another if the images were obtained outside of their physician's system. Patients must frequently even pay out of pocket for the creation of the disc [33]. With medical images or their hashes stored across a blockchain, images could be easily be shared among healthcare systems and providers.

Image sharing via a blockchain could occur either through a public (permissionless) or private (permissioned) blockchain. With a public blockchain, transactions could be appended to the blockchain which given permission to other hospital systems to view a patient's medical images. With a private blockchain, individual users (such as physicians) or groups (such as a hospital system), could be given permission to view images through transactions. Such an implementation could eliminate the need for medical imaging facilities to create and import discs and the need for patients to transport them, which may lead to repeat imaging and poor use of limited medical resources.

One particularly elegant model for blockchain-facilitated image sharing was proposed by Patel [17], in which three public/private key transactions on a blockchain enable secure image transfer by defining the source of the image, defining the corresponding owners (source and patient) of the image, and allowing access of the image from its source after verification. In this framework, an image is "published" as a public/private key set which is accessed by a private key held by the patient. The blockchain carrying these transactions is used to verify that a requesting party—such as a physician or another hospital—is included on a list permitted to access a particular imaging study, and that the particular study corresponds to these permissions.

There exist some platforms such as Cross-enterprise Document Sharing for Imaging (XDS-I) [23–26] and DICOMWeb [27] which enable the sharing of medical imaging studies across the Internet. Blockchain implementations for image sharing will not replace such standards but instead will supplement them. For instance, a commercially available medical image sharing platform, Nucleus.io, is implemented on the Ethereum network. Medical images are not stored within the blockchain itself. Instead, DICOMweb URLs are stored which allows patients to control access to their own data [34, 35]. Implementations such as this could potentially allow for patient-centered ownership of their own medical records [19], which are increasingly dependent upon imaging. If patients are in control of their own imaging data within a blockchain, they can easily grant permission to healthcare providers to view those enabling physicians outside of their current healthcare system access to their data and enable them to easily seek a second opinion. Since the data are stored in a blockchain, patients can be assured that the original data are immutable and unable to be altered.

The usage of encryption is facilitated by but not explicitly mandated by the DICOM standard [36]. As such, DICOM is uniquely dynamic enough to be incorporated into many different blockchain platforms.

Tracking Medical Devices

A common non-healthcare implementation of blockchain technology is supply chain management [37]. Within healthcare, blockchain has been proposed for the management of pharmaceutical supply chains [38, 39]. The principles of this utility can be applied to implanted medical devices and prostheses [31, 32], especially with respect to the capacity of the device, its date of placement, its longevity, or its compatibility. For example, many patients undergo inferior vena cava (IVC) filter placement and fail to recall the date or circumstances leading to its placement. While this has been mitigated to some extent with novel solutions like registries and even identifying bracelets, the ability to package device information with the patient's imaging data would ensure that this information is not lost, and can follow the patient to his or her next location of care. Ready access to this information could assist interventionalists in procedural planning, reduce the likelihood of redundant imaging for these procedures, and potentially preclude the need for secondary interventions. Other examples include MRI compatibility for miscellaneous medical implants, power-injection parameters for access implants and catheters, pacemaker firmware, or stent-graft measurements and material composition.

Research

Images or their metadata distributed across a decentralized blockchain could enable individual healthcare enterprises to control access to data while still allowing for collaboration and data sharing across different enterprises. Protected health information could be kept private while de-identified images could be shared.

Once images are committed to the blockchain, they cannot be changed (immutability). Since the data could be easily verified and traced back to the source (data provenance), replication of research studies would be more straightforward. As it stands, meta-analysis functions as a surrogate to validate reproducibility of findings or results across disciplines. Committing data and analyses to the blockchain could streamline this process, and potentially obviate the need for the cumbersome methodology currently employed: exhaustive PubMed or index manual searches which are pruned by inclusion and exclusion criteria. In a sense, all data immediately becomes metadata.

The immutability of the blockchain can increase transparency by offering built-in safeguard against data manipulation; collected data may immediately be encoded (and timestamped) with analysis to follow, preventing manipulation of data and reducing the ease to generate exaggerated or false conclusions—so called "beautification" of data, as already described [26]. This could also limit the influence of sponsors on research outcomes by removing them from the data stream.

Even more beneficial to research efforts is the power of the blockchain to pool documentation and bypass the participatory obstacles that now make multi-center trials for uncommon practices or rare diseases so daunting. For example, Chainscript [26] is a proof-of-concept streamlined consent process based on blockchain principles, which automatically seeks and verifies consent for updated protocols on a master document for trial participants.

Teleradiology

Teleradiology is inherently a distributed enterprise and amenable to application of a distributed technology such as blockchain. Medical Diagnostic Web (MDW) is a company which utilizes a blockchain as a means to distribute interpretation of medical image studies in a marketplace. Medical imaging professionals (e.g., radiologists, cardiologists, obstetrician-gynecologists) buy into the platform by purchasing exam interpretation credits which they can then use to select which studies they want to interpret. Only those with the appropriate level of training, credentialing, and licensure will be selected to interpret individual studies. The company also purportedly will enable more streamlined AI analysis of medical imaging studies [40].

Artificial Intelligence

Currently, most machine learning implementations rely upon centralized datasets and servers which put them at risk for alteration and data loss and therefore potentially spurious and untrustworthy outcomes. Decentralized artificial intelligence is a concept which combines machine learning algorithms with blockchain technology which allows the algorithms to consume data from and store output data within a distributed blockchain ledger [41]. Through distribution, the data can be "cryptographically signed, validated, and agreed on by all mining nodes" thus increasing data integrity and confidence in the inputs and outputs of the algorithms [42].

Blockchains could store multiple different kinds of patient data such as notes, lab values, data from wearable devices, precision medicine and genomic data, and medical imaging and make it available in de-identified batches for machine learning algorithms to consume for corroboration and correlation. Then, smart contracts could enable machine learning algorithms to be run every time a new imaging study is appended to the blockchain, approximating real-time analysis and augmentation.

At the Society for Imaging Informatics in Medicine's 2018 annual meeting, the Innovation Challenge People's Choice Award was given to a project entitled *Diagnosis Protocol - Using Blockchain to Accelerate Artificial Intelligence in Medical Imaging* [43]. The system enables patients, healthcare providers, and institutions to upload de-identified medical imaging data associated with the diagnosis, and it incentivizes people to do so via a tokenized reward with cryptocurrency [44].

References

1. Alexander A, McGill M, Tarasova A, Ferreira C, Zurkiya D. Scanning the Future of Medical Imaging. J Am Coll Radiol. 2018. [cited 2019 Mar 20]; Available from: http://www.sciencedirect.com/science/article/pii/S1546144018312821
2. Haber S, Stornetta WS. How to Time-Stamp a Digital Document. 13
3. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available from: https://bitcoin.org/bitcoin.pdf
4. Statement of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network, United States Department of the Treasury | FinCEN.gov. [cited 2018 Sep 20]. Available from: https://www.fincen.gov/news/testimony/statement-jennifer-shasky-calvery-director-financial-crimes-enforcement-network
5. Cryptocurrency Market Capitalizations | CoinMarketCap. [cited 2019 May 30]. Available from: https://coinmarketcap.com/
6. Swan M: Blockchain: Blueprint for a New Economy, 1st edition. Beijing, O'Reilly Media, 2015, 152 p
7. Gartner 2019 Hype Cycle for Blockchain Business Shows Blockchain Will Have a Transformational Impact across Industries in Five to 10 Years. Gartner. [cited 2019 Oct 9]. Available from: https://www.gartner.com/en/newsroom/press-releases/2019-09-12-gartner-2019-hype-cycle-for-blockchain-business-shows
8. There's No Good Reason to Trust Blockchain Technology. Wired. [cited 2019 Oct 30]; Available from: https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/
9. Busby M. Blockchain is this year's buzzword – but can it outlive the hype? The Guardian. 2018 Jan 30 [cited 2019 Oct 30];

Available from: https://www.theguardian.com/technology/2018/jan/30/blockchain-buzzword-hype-open-source-ledger-bitcoin
10. Wood DG. Ethereum: a secure decentralised generalised transaction ledger. 32.
11. Baran P. On Distributed Communications. 1964
12. Bach LM, Mihaljevic B, Zagar M. Comparative analysis of blockchain consensus algorithms. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2018. p 1545–50.
13. Definition of PROVENANCE. [cited 2019 Mar 20]. Available from: https://www.merriam-webster.com/dictionary/provenance
14. Tapscott D, Tapscott A: Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World, Reprint edition. Portfolio: New York, 2018, 432 p
15. Göbel J, Krzesinski AE. Increased block size and Bitcoin blockchain dynamics. In: 2017 27th International Telecommunication Networks and Applications Conference (ITNAC). 2017. p 1–6
16. Block size limit controversy - Bitcoin Wiki. [cited 2019 Oct 9]. Available from: https://en.bitcoin.it/wiki/Block_size_limit_controversy
17. Vazirani AA, O'Donoghue O, Brindley D, Meinert E: Implementing blockchains for efficient health care: systematic review. J Med Internet Res 21(2):e12439, 2019
18. Patel RP: Cloud computing and virtualization technology in radiology. Clin Radiol 67(11):1095–1100, 2012
19. Silva LAB, Costa C, Oliveira JL: A PACS archive architecture supported on cloud services. Int J Comput Assist Radiol Surg 7(3):349–358, 2012
20. Hostetter J, Khanna N, Mandell JC: Integration of a Zero-footprint Cloud-based Picture Archiving and Communication System with Customizable Forms for Radiology Research and Education. Acad Radiol 25(6):811–818, 2018
21. Awokola JA, Emuoyibofarhe JO, Meinel C, Ajala FA. Performance evaluation of a cloud-based picture archiving and communication system (PACS). 2019;7
22. Fedorov AK, Kiktenko EO, Lvovsky AI: Quantum computers put blockchain security at risk. Nature 563(7732):465, 2018
23. Li J, Li N, Peng J, Cui H, Wu Z: Energy consumption of cryptocurrency mining: a study of electricity consumption in mining cryptocurrencies. Energy:160–168, 2019
24. Ahram T, Sargolzaei A, Sargolzaei S, Daniels J, Amaba B. Blockchain technology innovations. In: 2017 IEEE Technology Engineering Management Conference (TEMSCON), 2017. p 137–41
25. Drosatos G, Kaldoudi E: Blockchain applications in the biomedical domain: a scoping review. Comput Struct Biotechnol J 17:229–240, 2019
26. Zhou L, Wang L, Sun Y: MIStore: a blockchain-based medical insurance storage system. J Med Syst 42(8):149, 2018
27. Can blockchain disrupt health education, licensing, and credentialling? | The Lancet Global Health Blog. [cited 2018 Oct 23]. Available from: http://globalhealth.thelancet.com/2017/10/31/can-blockchain-disrupt-health-education-licensing-and-credentialling
28. Jirgensons M, Kapenieks J: Blockchain and the future of digital learning credential assessment and management. J Teach Educ Sustain 20(1):145–156, 2018
29. Public Health Surveillance using Decentralized Technologies | Blockchain in Healthcare Today. [cited 2019 May 9]; **Available from:** https://blockchainhealthcaretoday.com/index.php/journal/article/view/17
30. Agbo CC, Mahmoud QH, Eklund JM: Blockchain Technology in Healthcare: A Systematic Review. Healthc Basel Switz 7, 2, 2019
31. Patel V: A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health Inform J 1: 1460458218769699, 2018
32. Image Share [Internet]. [cited 2019 Apr 15]. Available from: https://www.rsna.org/en/practice-tools/data-tools-and-standards/image-share-validation-program
33. Morin RL: Outside Images on CD: a management nightmare. J Am Coll Radiol 2(11):958, 2005
34. Applying Blockchain to Healthcare. Society for Imaging Informatics in Medicine; 2017 [cited 2019 Apr 15]. Available from: https://siim.org/page/17w_blockchain
35. How It Works. Nucleus.io. [cited 2019 Apr 15]. Available from: https://nucleus.io/how-it-works/
36. NEMA. DICOM PS3.15 2019d - Security and System Management Profiles [Internet]. [cited 2019 Oct 31]. Available from: http://dicom.nema.org/medical/dicom/current/output/html/part15.html
37. Wang Y, Singgih M, Wang J, Rit M: Making sense of blockchain technology: How will it transform supply chains? Int J Prod Econ 211:221–236, 2019
38. Tseng J-H, Liao Y-C, Chong B, Liao S: Governance on the drug supply chain via gcoin blockchain. Int J Environ Res Public Health 15(6):1055, 2018 Jun
39. Mackey TK, Nayyar G: A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expert Opin Drug Saf 16(5):587–602, 2017
40. A Link to a Better Marketplace? - Radiology Today Magazine. [cited 2019 Apr 25]. Available from: https://www.radiologytoday.net/archive/rt0119p16.shtml
41. Nebula AI Team. Nebula Ai (NBAI)- Decentralized ai Blockchain Whitepaper. 2018 [cited 2019 Apr 25]. Available from: https://icorating.com/upload/whitepaper/GhqtZKXl3L5J5TgWS6ZO0oTzpRjwDE5KrwKSdy9L.pdf
42. Salah K, Rehman MHU, Nizamuddin N, Al-Fuqaha A: Blockchain for AI: review and open research challenges. IEEE Access 7: 10127–10149, 2019
43. 2018 SIIM Innovation Challenge - Past Winners - Society for Imaging Informatics in Medicine. SIIM.org. [cited 2019 Apr 15]. Available from: https://siim.org/page/18innovation_past
44. Blockchain project wins 'People's Choice' award at national medical conference | UIC Today. [cited 2019 Apr 25]. Available from: https://today.uic.edu/blockchain-project-wins-peoples-choice-award-at-national-medical-conference