Journal of the American Medical Informatics Association, 24(6), 2017, 1211–1220
doi: 10.1093/jamia/ocx068
Advance Access Publication Date: 8 September 2017
Review

Review

Blockchain distributed ledger technologies for biomedical and health care applications

Tsung-Ting Kuo,[1] Hyeon-Eui Kim,[1] and Lucila Ohno-Machado[1,2]

[1]UCSD Health Department of Biomedical Informatics, University of California San Diego, La Jolla, CA, USA and [2]Division of Health Services Research and Development, Veterans Administration San Diego Healthcare System, La Jolla, CA, USA

Corresponding Author: Lucila Ohno-Machado, 9500 Gilman Dr, San Diego, CA 92130, USA. E-mail: lohnomachado@ucsd.edu; Phone: +1 (858) 822-4931.

Received 22 February 2017; Revised 22 May 2017; Accepted 30 June 2017

ABSTRACT

Objectives: To introduce blockchain technologies, including their benefits, pitfalls, and the latest applications, to the biomedical and health care domains.
Target Audience: Biomedical and health care informatics researchers who would like to learn about blockchain technologies and their applications in the biomedical/health care domains.
Scope: The covered topics include: (1) introduction to the famous Bitcoin crypto-currency and the underlying blockchain technology; (2) features of blockchain; (3) review of alternative blockchain technologies; (4) emerging nonfinancial distributed ledger technologies and applications; (5) benefits of blockchain for biomedical/health care applications when compared to traditional distributed databases; (6) overview of the latest biomedical/health care applications of blockchain technologies; and (7) discussion of the potential challenges and proposed solutions of adopting blockchain technologies in biomedical/health care domains.

Key words: blockchain, distributed ledger technology, health information exchange, security, interoperability

THE BITCOIN BLOCKCHAIN

The Bitcoin crypto-currency

One of the best-known applications of blockchain is the crypto-currency Bitcoin (in this article, we use "Bitcoin" to indicate the currency and "bitcoin" to denote the actual digital coins).[1,2] Bitcoin was proposed by the unidentified person or persons "Satoshi Nakamoto" (which is speculated to be a fake name) through a famous white paper[1] published in October 2008. In the following year, the open-source Bitcoin implementation was released.[2] As a peer-to-peer digital currency without a central administrator, Bitcoin is categorized as a decentralized virtual currency by the US Treasury.[3] Bitcoin has the unofficial ISO-4217 currency code XBT, which is used by organizations and companies such as Bloomberg[4] and XE.[5] The unit of Bitcoin is BTC, and 1 BTC is equivalent to about 1200 US dollars as of April 2017.[6] Currently, Bitcoin has the highest total market value (19 billion US dollars or 16 million BTC, as of April 2017) among >100 various crypto-currencies currently being used.[7] Bitcoins (BTCs) can now be used online at electronic commerce websites to purchase a wide range of commodities and services (see Supplementary Appendix Section A.1 for more details).[8–11]

Known challenges for crypto-currencies: double-spending and single-point-of-failure

The underlying distributed ledger technology of Bitcoin is also indicated as the Bitcoin blockchain, to distinguish it from other blockchain technologies. The original motivation of the Bitcoin blockchain technology was to solve the peer-to-peer double-spending problem (Figure 1)[1]: How can we prevent electronic coins (defined as "a chain of digital signatures"[1]) such as bitcoins from being spent twice without having a central intermediary (eg, bank or mint)?

It should be noted that the central intermediary is not desired because it creates a single-point-of-failure, as shown in Figure 2A.[12] That is, if the central intermediary is down for any reason, including scheduled maintenance, the entire network system stops. Also, if the

central intermediary is intruded upon (eg, the administrator account is compromised), the whole network faces the invasion risk.[13] Therefore, a decentralized network topology, as shown in Figure 2B, would be more desirable to avoid such a single-point-of-breach.

The Bitcoin blockchain solution: hash-chain timestamping and proof-of-work algorithm

To solve the double-spending problem, each computation node in the blockchain network not only needs to store every transaction to enable the distributed verification of the transactions, but also to follow a distributed timestamp mechanism to determine which transactions should be accepted and which should be rejected, as shown in Figure 2C. The Bitcoin blockchain exploits hash-chain[14] as a distributed timestamp mechanism, and every node maintains a copy of the chain to store every transaction (Figure 3).

Additionally, the "mining" process (ie, creating a block with enclosed transactions) should be relatively difficult to do, but relatively easy to check.[15] The process should be difficult (ie, time-consuming and costly) in order to make attempts to create invalid blocks prohibitively expensive (at the cost of increasing the time available to create valid blocks). To implement such a design, Bitcoin blockchain adopts a proof-of-work protocol[1] that each block creator has to follow. Figure 4 illustrates how a chain of blocks is created with this protocol.[16,17]

An additional benefit of the proof-of-work consensus protocol used in blockchain is the ability to resolve disagreement of the chains, and thus let blockchains be immutable audit trails.[1,15] That is, when an attacker modifies a block, all the blocks after that block are recomputed, because each block contains the hash value of the previous block's header,[16] and the computational cost of such modification should be high enough to prohibit attacks (Figure 4).

On the other hand, when an attacker creates a malicious chain to compete with an honest chain and tries to replace the honest one, the proof-of-work majority voting mechanism can also significantly reduce the probability of such an attack to succeed (Figure 5). Detailed analyses of the attack-resisting ability of the blockchain proof-of-work consensus protocol are proposed in several recent studies.[1,18–22] The Bitcoin mechanism also provides rewards to the nodes, as an incentive to compensate the high cost associated with "mining" a new block and verifying transactions (see Supplementary Appendix Section A.2 for more details).

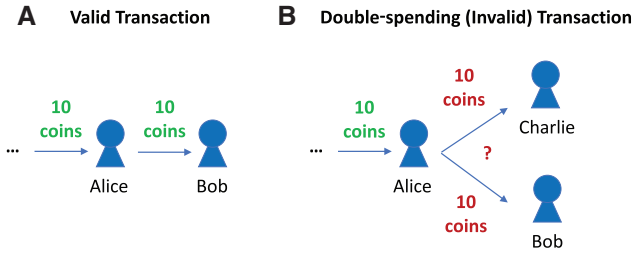

Figure 1. The problem of double-spending without a central intermediary. (**A**) Valid transaction. (**B**) Double-spending (invalid) transaction. The problem illustrated in this example is: Suppose Alice has 10 coins and then sends all 10 coins to Bob. How can Bob (and other people using the coin) know that Alice has not sent the same 10 coins to Charlie before, without having a bank to verify transactions?

ALTERNATIVE BLOCKCHAIN TECHNOLOGIES AND BLOCKCHAIN APPLICATIONS BEYOND THE FINANCIAL DOMAIN

Alternative crypto-currencies and blockchains

After Bitcoin, many other crypto-currencies, such as Ethereum (4 billion USD market cap),[23–25] Ripple (1 billion USD market cap),[26,27] Dash (534 million USD market cap),[28,29] Litecoin (512 million USD market cap),[30,31] and Monero (311 million USD market cap) were developed.[32,33] (These market caps are as of April 2017.[7]) Additionally, several alternative blockchains (or "altchains") have been proposed (such as Colored Coins[34,35] and Sidechains[36]) and are considered to be blockchain 1.0 technologies.[37] Several alternative protocols to the proof-of-work (see the example shown in Figure 4)

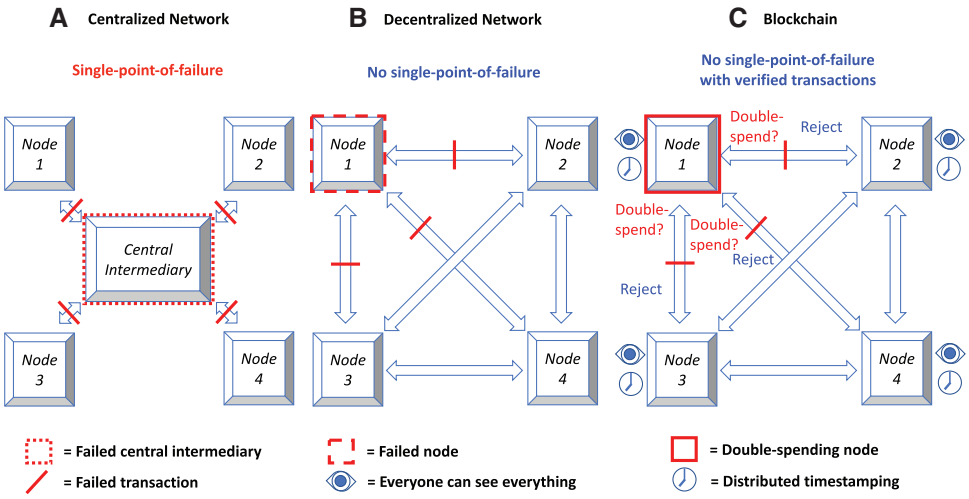

Figure 2. Comparison of the distributed network topologies. (**A**) Centralized network topology, which creates a single-point-of-failure (the central intermediary). If the central intermediary is down or attacked, the entire network stops working. (**B**) Decentralized network topology, which does not contain single-point-of-failure. If one of the nodes, such as *Node 1*, is down or attacked, the rest of the network can still operate normally. (**C**) Blockchain. If "everyone can see everything" and there exists a distributed timestamp mechanism, the double-spending problem can be solved on such a decentralized network. In the example illustrated in Figure 1, if everyone (ie, Alice, Bob, Charlie, and all other people in the same network) knows that Alice (*Node 1* in this example) sent 10 coins to Charlie yesterday, the transaction to send the same 10 coins to Bob today can thus be rejected through a verification process without consulting a bank.

have also been proposed, such as proof-of-stake, where the node with oldest coins can create a new block[38–40]; proof-of-burn, where the node willing to "burn" or destroy the largest number of coins, by sending it to a "NULL" address, can create a new block[41,42]; and proof-of-elapsed-time, where the node with the shortest wait time verified by the trusted execution environment can create a new block.[43,44]

Blockchains as distributed ledgers

Although blockchain was originally designed as a crypto-currency, it is also regarded as a new form of the distributed database or ledger, as arbitrary data can be stored in the metadata of the transactions. Bitcoin blockchain supports metadata since 2014.[45–48] The original Bitcoin blockchain only supports 80 bytes of metadata, but other blockchain implementations support larger sizes. For example, MultiChain[46,49] supports metadata with adjustable size, and BigchainDB[45,50] has no hard limit on metadata size.

A blockchain-based distributed ledger is also known as blockchain 2.0,[37] including the new technologies of "smart properties" and "smart contracts."[23,24,34,36,37,51–56] The former refers to the digital properties with ownership controlled by blockchain, and the latter refers to the computer programs designed to manage smart properties. One of the most well-known smart property/contract systems is Ethereum,[23–25] which is a decentralized platform for smart contracts.[23,24] Ethereum as a crypto-currency itself also has the second-largest market cap as of April 2017.[7] Microsoft adopted Ethereum as the core of its new Blockchain-as-a-Service on the Azure cloud computing environment.[57] Additional distributed ledger blockchains are described in Supplementary Appendix Section A.3.

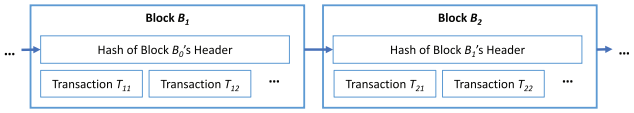

Figure 3. An example of simplified blockchain (hash-chain). Each transaction of coins is enclosed in a *block*. A block may contain multiple transactions and is a basic unit to be verified. Each block also contains a hash value of the previous block's header, and thus forms a *hash-chain* or *blockchain*. As all blocks are chained, the order of the blocks is deterministic; therefore, each block can serve as a timestamp of the enclosed transactions to solve the double-spending problem. Note that each node maintains a copy of the whole blockchain, thus every node can verify every transaction. For example, suppose the transaction from Alice to Charlie is enclosed in block B_1 and the one from Alice to Bob is enclosed in block B_2; everyone in the network can verify that B_1 happened before B_2 by checking the hashed blockchain, and thus the double-spend transaction from Alice to Bob should be rejected.

Nonfinancial applications for the original and alternative blockchain technologies

Recently, the idea of blockchain 3.0 has been proposed to denote nonfinancial applications of the distributed ledger technology.[37] For example, Namecoin applies Bitcoin technology to Domain Name Server and identity management.[58,59] Another example is to apply blockchain in the scientific research cycle (eg, funding, experiment, analysis, publication, etc.), as blockchain is decentralized, distributed, immutable, and transparent.[60] These applications are implemented either as permission-less (ie, any user can participate) or permissioned (ie, only authorized institutions or researchers can participate) blockchain networks.

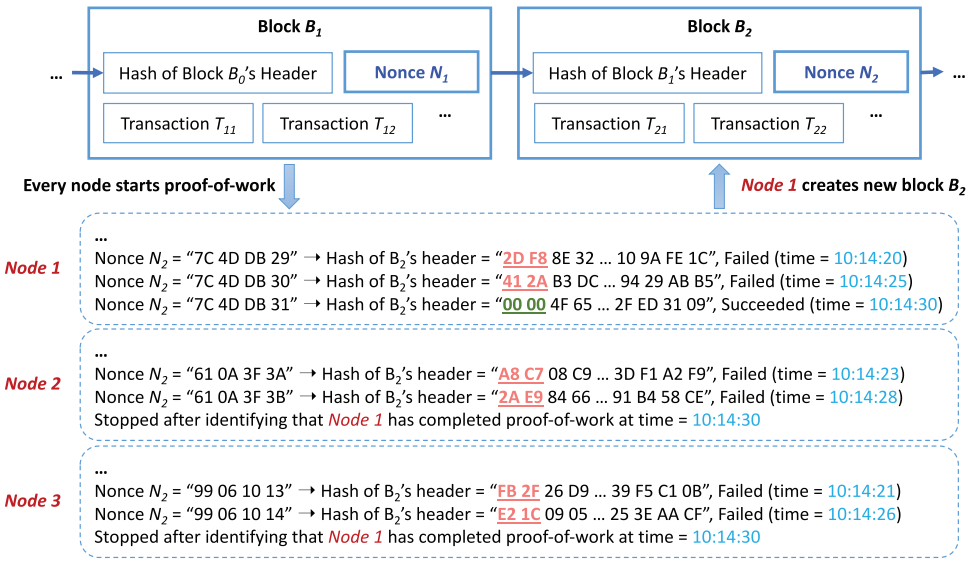

Figure 4. An example of the nonce mechanism for the *proof-of-work* protocol. Each block contains an additional "nonce" (32-bit or 8-hex-digits in this example), which is a counter that serves as one of the inputs of the hashing function. To "proof" the hashing work, the nonce is incremented by one bit each time for the hash computation (ie, the "work"), until the hashed value (256-bit or 64-hex-digits in this example) contains a predefined number of leading zero bits (ie, "proof" of the work, 16-bit or 4-hex-digits in this example). Meanwhile, the newly generated unconfirmed transactions are collected in a memory pool on each node. The first node that successfully completes the *proof-of-work* (*Node 1* at 10:14:30 in this example) has the privilege to create a new block (B_2 in this example), verify the transactions, move the confirmed transactions from the memory pool to a newly created block, and add the block to the end of the longest chain (if there are competing chains). It also gets paid (eg, 12.5 bitcoins) for this work. Also, the remaining nodes (*Nodes 2* and *3* in this example) stop the *proof-of-work* mining for B_2 when *Node 1* completes the *proof-of-work*. This way, the mining process becomes difficult (ie, one needs to compute the difficult hashing problem by trying different "nonce" values), while the checking process remains easy (ie, just one hash to see if the predefined leading bits are all zeroes). In our example, Alice cannot easily create an invalid block for her double-spend transaction, while Bob and Charlie can easily check that the block Alice created is invalid. It should be noted that the system clocks on the nodes may not be synchronized, therefore we use a global time for demonstration purposes in this example. Also note that, if an attacker modifies any of the transactions in block B_1, the value of "hash of block B_1's header" and thus block B_2 need to be recalculated, and consequently all blocks after B_1 (ie, B_2 B_3, B_4, B_5,...) also need to be recomputed. Therefore, the computational cost of attacking becomes prohibitively high.

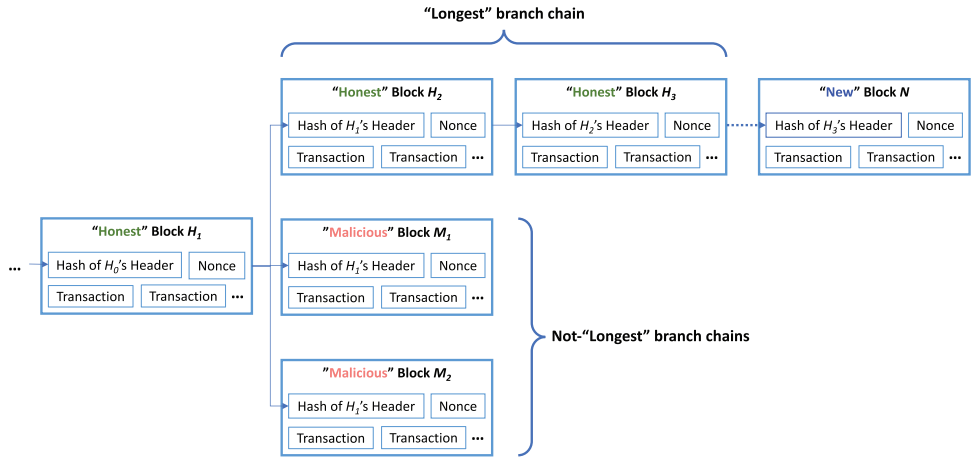

Figure 5. An example of how Bitcoin blockchain deals with branching chains. In this scenario, attackers create malicious blocks (M_1 and M_2) to compete with an honest block (H_2), in an attempt to take over the honest chain (H_1 and all blocks before). Assuming the computational power of honest nodes is *larger* than that of malicious nodes, an *honest* block H_3 is created right after H_2, before the attackers create new malicious blocks after M_1 and M_2. Based on the blockchain mechanism, each node first identifies a valid block based on the length of the chain, and creates a new block (N) only at the end of the *longest* chain ($H_1 \rightarrow H_2 \rightarrow H_3$ in this example) while ignoring shorter chains ($H_1 \rightarrow M_1$ and $H_1 \rightarrow M_2$ in this example). In other words, the blockchain that has been worked on most wins the competition (ie, majority voting of "one CPU, one vote,"[1] since the longest blockchain represents the majority decision of block creators). Given that the mining process is expensive and the honest nodes have higher computational power (ie, have more CPU "voters") than the malicious nodes, the probability for the attacker to successfully modify a block and all blocks thereafter (ie, create a malicious competing chain) is very small.

Although blockchain technologies such as Bitcoin blockchain are widely recognized and have been used for several purposes, in health care they became known as a means to pay ransom for institutions that had their data "kidnapped" (ie, encrypted by malicious users who request payment to unencrypt the data).[61,62] Ransomware has affected several health care systems, resulting in thousands of dollars in known ransom payments so far. Bitcoin currency is used because it is reliable, while it is very difficult to track its recipient. The technology behind Bitcoin, however, can be used to help instead of harm health systems and biomedical research.

KEY BENEFITS OF BLOCKCHAIN WHEN COMPARED TO TRADITIONAL DISTRIBUTED DATABASES FOR BIOMEDICAL/HEALTH CARE APPLICATIONS

To better understand why blockchain distributed ledger technology may be feasible for biomedical and health care applications, we describe the key benefits or comparative advantages of blockchain[45,46,63–65] by comparing it with the traditional distributed database management system (DDBMS),[66,67] such as Structured Query Language (SQL)-based systems like Oracle[68] and NoSQL-based systems like Apache Cassandra.[69]

The first key benefit of blockchain is *decentralized management*. DDBMSs are logically centralized-managed (ie, users logically feel they are operating a centralized database, but the underlying machines can be physically distributed), while blockchain is a peer-to-peer, decentralized database management system (ie, each node runs independently while following the protocols).[45,63,64] Therefore, blockchain is suitable for applications where independently managed biomedical/health care stakeholders (eg, hospitals, providers, patients, and payers) wish to collaborate with one another without ceding control to a central management intermediary.[13,45,65]

The second key benefit is the *immutable audit trail*. DDBMSs support create, read, update, and delete functions like all database systems, while blockchain only supports create and read functions (ie, it is very difficult to change the data or records).[45] Thus, blockchain is suitable as an unchangeable ledger to record critical information (eg, insurance claim records).

The third is *data provenance*. On DDBMS, the ownership of digital assets can be modified by the system administrator, while on blockchain, the ownership can only be changed by the owner, following the cryptographic protocols.[45] Also, the origins of the assets are traceable (ie, the sources or the data and records can be confirmed),[45] increasing the reusability of verified data (eg, for insurance transactions).[70] Therefore, blockchain is suitable for use in managing critical digital assets (eg, patient consent records).

The fourth benefit is both *robustness* and *availability*. Although DDBMS and blockchain are based on distributed technology and thus do not suffer from single-point-of-failure, it would be costly for DDBMS to achieve the high level of data redundancy blockchain does (ie, each node has a whole copy of whole historical data records).[64] Thus, blockchain is suitable when the preservation and continuous availability of records (eg, the electronic health records of patients) are important.

The final key benefit of blockchain is related to the improved *security* and *privacy* using cryptographic algorithms. For example, Bitcoin blockchain utilizes the 256-bit Secure Hash Algorithm (SHA-256), a cryptographic hash function defined in the US Federal Information Processing Standards 186-4, published by the National Institute of Standards and Technology,[71] as the cryptographic hash function in the hash-chain that the proof-of-work algorithm runs on.[72] SHA-256 is also used to generate user addresses for privacy/anonymity improvement (ie, each user is represented by a hash value instead of a real identity, such as an IP address).[72] Furthermore, Bitcoin blockchain exploits the 256-bit Elliptic Curve Digital Signature Algorithm, an asymmetric cryptography algorithm defined in the US Federal Information Processing Standards 180-4,[73] to generate and verify high-security-level public and private keys as digital signatures, and thus ensures ownership of the digital assets, as with patient records.[74]

To summarize, the key benefits for adopting blockchain technology in biomedical and health care applications include: (1) decentralized management, (2) immutable audit trail, (3) data provenance, (4) robustness/availability, and (5) security/privacy.

Table 1. Blockchain benefits and uses cases to improve medical record management

Blockchain: Key Benefit	Biomedical/Health Care Use Case: Improved Medical Record Management
Decentralized Management	Patient-managed health care records: "*[Patient] becomes the platform, owning and controlling access to their healthcare data. This removes all obstacles to patients acquiring copies of their healthcare records or transferring them to another healthcare provider.*"[85]
Immutable Audit Trail	Unalterable patient records: "*The data are stored in the private blockchain cloud. Blockchain may guarantee medical data cannot be changed by anybody including physicians and patients himself/herself internally and natively.*"[77]
Data Provenance	Source-verifiable medical records: "*Records are signed by source, allows legitimacy of records to be verified (and false records to be plausibly denied).*"[78]
Robustness/Availability	Reduced risk of patient recordkeeping: "*Because data is stored on a decentralized network, there is no single institution that can be robbed or hacked to obtain a large number of patient records.*"[85]
Security/Privacy	Increased safety of medical records: "*Data is encrypted in the blockchain and can only be decrypted with the patient's private key. Even if the network is infiltrated by a malicious party, there is no practical way to read patient data.*"[85]

Table 2. Blockchain benefits and use cases to enhance insurance claim process

Blockchain: Key Benefit	Biomedical/Health Care Use Case: Enhanced Insurance Claim Process
Decentralized Management	Real-time claim processing: "*The ability to remove intermediaries from a process is the capability that sets Blockchain apart from other technologies. This capability will allow the solution to facilitate real-time claims adjudication by replacing the health plan intermediation with transparent Blockchain technologies.*"[94]
Immutable Audit Trail	Improved claim auditing and fraud detection: "*Payer, private and government insurers, and individual payers have the benefits of] audits facilitation and better fraud detection [based on Blockchain immutability].*"[92]
Data Provenance	Verifiable records for claim qualification: "*[The chief obstacle of the claim qualification process] is the distributed nature of the many records that feed the decisions of patients, providers, and Medicaid administrators. . . The requirements for verification. . . are precisely the obstacles that a distributed blockchain solution. . . can address.*"[95]
Robustness/Availability	Enhanced accessibility of patient data: "*[Provider, health-related services and medical goods have the benefits of] patient data accessible from multiple silos [based on Blockchain virtual ledger].*"[92]
Security/Privacy	Increased security of patient medical insurance information: "*[Member/patient have the benefits of] less likelihood of hacking of. . . financial information [based on Blockchain mechanism].*"[92]

BLOCKCHAIN TECHNOLOGIES FOR BIOMEDICAL/HEALTH CARE APPLICATIONS

As the benefits of blockchain described above are crucial for biomedical and health care applications, health care has become one of the most important emerging application areas of the blockchain distributed ledger technology.[65] In general, blockchain is treated as a distributed ledger to store health care–related data for sharing, exchanging, analyzing, recording, and validating purposes among stakeholders.[13,65,75–106]

Among the biomedical/health care applications, the one most discussed is related to the adoption of blockchains as an underlying infrastructure for Health Information Exchange (HIE), or health transactions between patients, providers, payers, and other relevant parties.[13,75–98] These applications can further be categorized based on their main goals to exploit the blockchain-stored data, and are described in the Improved medical record management, Enhanced insurance claim process, and Accelerated clinical/biomedical research sections. The applications beyond HIE are depicted in the Advanced biomedical/health care data ledger section. For each category of application, we further discuss the use cases and key benefits of adopting blockchain technology.

Improved medical record management

Many studies or ongoing projects focus on exchanging patient care data using blockchains to improve medical record management,[75,76] including Healthcare Data Gateways,[77] MedVault,[78] Fatcom,[79] BitHealth,[80] Gem Health Network,[81] and others.[82–87,96,97] Several well-known companies, such as Deloitte[88] and Accenture,[89] are also involved in applying blockchain technology to store health care data and manage medical records. Another famous example is Guardtime,[90] a company providing a blockchain-based system in Estonia to secure 1 million health records.[91] The benefits and use cases of adopting blockchain to improve medical record management are summarized in Table 1.

Enhanced insurance claim process

Another important goal is to verify the claim transactions to support health care financing tasks (ie, health plan claims), such as preauthorization payment,[92] alternative payment models,[93] automatic claims using Fast Healthcare Interoperability Resources[107] and smart contract,[94] and Smart Health Profile to help manage the constant exit and reentry of Medicaid beneficiaries due to eligibility changes.[95] The benefits and use cases of adopting blockchain to enhance insurance claim process are summarized in Table 2.

Accelerated clinical/biomedical research

Several researchers also propose accelerating secondary use of clinical data (ie, clinical and biomedical studies and research) using blockchain technology, including MedRec,[96,97] Data Lake,[86] Healthbank,[76,102] and blockchain-based data sharing networks.[98] Also, ModelChain adopted blockchain to increase the security and

Table 3. Blockchain benefits and use cases to accelerate clinical/biomedical research

Blockchain: Key Benefit	Biomedical/Health Care Use Case: Accelerated Clinical/Biomedical Research
Decentralized Management	Improved care data sharing and analysis without ceding control: "*Blockchain is by design a decentralized (ie, a peer-to-peer, non-intermediated) architecture… Each institution can keep full control of their own computational resources [while collaborating with other institutions for data sharing and analysis].*"[13]
Immutable Audit Trail	Trackable and timestamped patient-generated data: "*Using Blockchain, this model could be even further individualized in a way that personal patient-generated health data which is available to researchers can be tracked in the research process with a timestamp.*"[76,102]
Data Provenance	Evidenced provenance for medical research data: "*The MedRec [Blockchain-based prototype for electronic health records and medical research data is]… enabled with crucial properties of provenance.*"[96,97]
Robustness/Availability	Superior health care data availability: "*Blockchain would ensure continuous availability and access to real-time data. Real-time access to data would improve clinical care coordination and improve clinical care in emergency medical situations. Real-time data would also allow researchers and public health resources to rapidly detect, isolate and drive change for environmental conditions that impact public health. For example, epidemics could be detected earlier and contained.*"[86]
Security/Privacy	Secured and privacy-preserving health care data sharing: "*Utilization of the… health blockchain… has the potential to engage millions of individuals, health care providers, health care entities and medical researchers to share vast amounts of genetic, diet, lifestyle, environmental and health data with guaranteed security and privacy protection.*"[86]

Table 4. Blockchain benefits and use cases to advance biomedical/health care data ledger

Blockchain: Key Benefit	Biomedical/Health Care Use Case: Advanced Biomedical/Health Care Data Ledger
Decentralized Management	Decentralized health data backbone: "*The blockchain then becomes the backbone for digital health, incorporating data from patient-based technologies and the EMR to provide a… pool from which authorized users, such as providers and patients, has access. All of the data is stored in a decentralized manner, with no single entity storing or having singular authority to access.*"[101]
Immutable Audit Trail	Unchangeable log of clinical research protocols: "*Use of blockchain technology has recently been shown to provide an immutable ledger of every step in a clinical research protocol, and this could easily be adapted to basic and experimental model science. All participants in the peer-to-peer research network have access to all of the time stamped, continuously updated data. It is essentially tamper proof since any change, such as to the prespecified data analysis, would have to be made in every computer (typically thousands) within the distributed network.*"[104]
Data Provenance	Ensure original manufacturer and ownership transferring in pharmaceutical supply chain: "*Using Blockchain, the origin of the [medicine] product and its components are detected, and any transfer of ownership in each case is made clear and available to everyone. Forged, poor quality or stolen goods can be tracked and identified.*"[76,105]
Robustness/Availability	Improved robustness for counterfeit drug prevention/detection systems in pharmaceutical supply chain: "*In the existing solutions, there is still a central authority that can be compromised and documents that can be faked… If [the current solutions] can be modified with blockchain-enabled anti-tampering capabilities during manufacturing, the supply and dispensation system could make drug counterfeiting a non-issue.*"[92]
Security/Privacy	Higher patient confidence in consent recording systems: "*Patients are able to add consent statements at any point in their care journey – confident that the blockchain will hold them securely.*"[89]

robustness of the distributed privacy-preserving health care predictive modeling across multiple institutions.[13] The benefits and use cases of adopting blockchain to accelerate clinical/biomedical research are summarized in Table 3.

Advanced biomedical/health care data ledger

Besides exploiting blockchains as ledgers of patient care data (ie, HIE), many studies and projects have also proposed using them to store various types of health care–related data, such as genomic and precision medicine data,[99,100] patient-centered or patient-related outcomes data,[101] provider/patient directories and care plans data,[93] clinical trial data,[92,103,104] patient consent data,[89] pharmaceutical supply chain data,[92,105] and biomarker data.[106] The benefits and use cases of adopting blockchain to advance biomedical/health care data ledger are summarized in Table 4.

POTENTIAL CHALLENGES AND PROPOSED SOLUTIONS FOR ADOPTING BLOCKCHAIN TECHNOLOGY FOR BIOMEDICAL/HEALTH CARE APPLICATIONS

Potential problems and challenges

There are several potential challenges to be considered when adopting blockchain technology in the biomedical/health care domain.

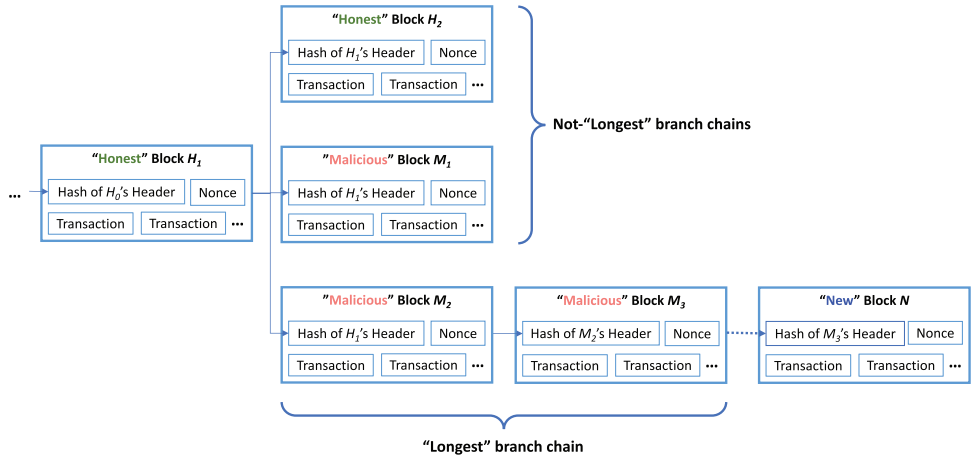

Figure 6. An example of 51% attack. In this scenario, attackers create malicious blocks (M_1 and M_2) to compete with an honest block (H_2), trying to take over the honest chain (H_1 and all blocks before). However, this time the computational power of host nodes is *smaller* than that of malicious nodes (ie, malicious nodes control more than 51% of the computing power on the network), thus a *malicious* block M_3 is created right after M_2. Based on the blockchain mechanism, the new block (N) will be created only at the end of the *longest* chain ($H_1 \rightarrow M_2 \rightarrow M_3$ in this example). Therefore, the attacker has successfully modified the blockchain record (from H_2 to M_2) and takes over the chain by winning the majority vote.

The first challenge is related to *transparency* and *confidentiality*. As "everyone can see everything" on a blockchain network,[46,110,109] heightened transparency and decreased confidentiality, such as open transparency of information during transfer, is usually considered a limitation of blockchain. Also, even if a user is "anonymized" by using hash values as addresses, the user may still be reidentified through inspection and analysis of the publicly available transaction information on the blockchain network, and therefore the blockchain network only provides "pseudonymity."[110–113] This issue is critical for biomedical/health care applications, because patient-related data (protected health information, or PHI, and personal identifiable information) are highly sensitive.

The second challenge is related to *speed* and *scalability*. The transaction time of blockchain can be long, depending on the protocol, and such a speed constraint may limit the scalability of blockchain-based applications. For example, with the proof-of-work protocol, there are about 288 000 transactions per day (or about 3.3 transactions per second) on average for Bitcoin due to the required computation workload, while there are 150 million transactions per day (or about 2000 transactions per second) on average for a credit card like Visa.[114,115] The theoretical maximum transaction speed for Bitcoin is 7 transactions per second due to the 1 megabyte block size limitation in the current protocol, while the theoretical maximum number of transactions is 4000 per second for Visa.[114,115] This issue is important when constructing real-time and scalable blockchain-based health care/biomedical applications.[89]

The last challenge is the *threat of a 51% attack*. A blockchain network may suffer from the "51% attack,"[23,46,116] which happens when there are fewer honest nodes than malicious ones in the whole network, and thus the whole network is taken over by the malicious attackers (Figure 6). This issue is also critical for security-demanding health care/biomedical applications.

Proposed solutions and implementations

The above challenges can be mitigated by careful design and implementation of the biomedical/health care application systems. We take ModelChain[13] as an example. ModelChain adopts blockchain to securely and robustly disseminate privacy-preserving predictive models (ie, a set of machine learning parameters or aggregated values) between health care institutions. Because it only disseminates predictive models but not PHI, transparency is not a critical issue. Also, it contains a machine learning process that can take a long time to run (minutes, or even hours), thus the transaction speed of blockchain becomes relatively negligible. Finally, since it adopts permissioned blockchain networks, malicious nodes could not arbitrarily participate in the network, and therefore the risk of a 51% attack is minimal.

Other implementation techniques to mitigate the *transparency/confidentiality* issue include encrypting sensitive data (eg, PHI or personal identifiable information) on the blockchain network,[87,97,118] storing sensitive data off-blockchain and only disseminating "pointers" (eg, encrypted links) or permission information on-blockchain,[88,96,97,117] and automating data management protocols using smart contracts.[96–98]

To deal with the *speed/scalability* issue, plausible solutions include exploiting blockchain as an index of health data instead of the repository of all records,[86] and storing only ongoing verified transactions rather than the complete history on blockchain.[92] Also, several new blockchain implementations, such as BigchainDB,[45,50] provide significantly higher transaction speed than the Bitcoin blockchain, which could also solve the speed and scalability problem.[18,119]

The threat of a 51% attack on the biomedical/health care blockchain network can be drastically reduced by using a virtual private network to disseminate the data and deploying some components of the system on private Health Insurance Portability and Accountability Act–compliant cloud computing environments such as iDASH (integrating Data for Analysis, Anonymization, and Sharing).[120,121]

CONCLUSION

We introduced Bitcoin and the underlying blockchain technology, which provides decentralized management, an immutable audit trail, data provenance, robustness/availability, and security/privacy. We contrasted blockchain technologies (ie, blockchain 1.0, 2.0, and 3.0), identified benefits of blockchain compared to traditional distributed databases for biomedical/health care applications, and provided an overview of the latest biomedical/health care applications of blockchain

technology (ie, improved medical record management, enhanced insurance claim process, accelerated clinical/biomedical research, and advanced biomedical/health care data ledger). There are several known potential challenges to adopting blockchain technologies (eg, transparency/confidentiality, speed/scalability, and the threat of a 51% attack). However, these challenges can be addressed through careful application design and implementation, therefore health care applications of blockchain continue to increase. Blockchain distributed ledger technology can advance the biomedical and health care domains in various novel ways, and we expect many new applications to emerge soon.

FUNDING

The authors are funded by the National Institutes of Health (U24AI117966) and the Patient-Centered Outcomes Research Institute (CDRN-1306-04819). The statements in this article are solely the responsibility of the authors and do not necessarily represent the views of PCORI, its Board of Governors or Methodology Committee. LO-M is funded by the National Institutes of Health (U54HL108460) and VA (IIR12-068). Research reported in this publication was supported by the National Human Genome Research Institute of the National Institutes of Health under Award Number K99HG009680. The content is solely the responsibility of the authors and does not necessarily represent the official views of the National Institutes of Health.

COMPETING INTERESTS

The authors have no competing interests to declare.

CONTRIBUTORS

T-TK conducted the literature review and drafted the manuscript. HK added critical discussion points and edited the manuscript. LO-M was principal investigator of this study; she provided the original idea, overall supervision of this study, and critical editing of the manuscript.

SUPPLEMENTARY MATERIAL

Supplementary material is available at *Journal of the American Medical Informatics Association* online.

REFERENCES

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. 2008. Accessed July 30, 2016.
2. Davis J. *The Crypto-currency: Bitcoin and Its Mysterious Inventor*. The New Yorker. http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency. Accessed January 11, 2017.
3. Calvery JS. *Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury*. Vienna, Virginia, United States: Financial Crimes Enforcement Network; 2013.
4. Dillet R. *Bitcoin Ticker Available On Bloomberg Terminal For Employees*. TechCrunch. https://techcrunch.com/2013/08/09/bitcoin-ticker-available-on-bloomberg-terminal/. Accessed December 14, 2016.
5. XE.COM INC. Currency Encyclopedia - XBT Bitcoin. http://www.xe.com/currency/xbt-bitcoin. Accessed February 15, 2017.
6. CoinDesk. Bitcoin Price. http://www.coindesk.com/price/. Accessed April 13, 2017.
7. CoinMarketCap. *Crypto-Currency Market Capitalizations*. https://coinmarketcap.com/. Accessed April 13, 2017.
8. Draupnir M. *What Can You Buy with Bitcoin*. WeUseCoins. https://www.weusecoins.com/what-can-you-buy-with-bitcoin/. Accessed December 14, 2016.
9. CoinDesk. *What Can You Buy with Bitcoin*. http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/. Accessed December 14, 2016.
10. Coinbase.com. *Where Can I Spend Bitcoin*. https://support.coinbase.com/customer/portal/articles/1834716. Accessed December 14, 2016.
11. Hughes M. *What Are Bitcoins Actually Used For Now in 2016*. MakeUseOf. http://www.makeuseof.com/tag/bitcoins-actually-used-now-2016/. Accessed December 14, 2016.
12. Fromknecht C, Velicanu D, Yakoubov S. A decentralized public key infrastructure with identity retention. *IACR Cryptology ePrint Archive*. 2014;2014:803.
13. Kuo T-T, Hsu C-N, Ohno-Machado L. ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
14. Lamport L. Password authentication with insecure communication. *Commun ACM* 1981;24(11):770–72.
15. Kelsey J. Introduction to Blockchains. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
16. Bitcoin.org. Bitcoin Developer Guide. https://bitcoin.org/en/developer-guide. Accessed February 1, 2017.
17. Blockchain Luxembourg S.A. *Unconfirmed Transactions: Live Updating List of New Bitcoin Transactions*. https://blockchain.info/unconfirmed-transactions. Accessed February 10, 2017.
18. Garay J, Kiayias A, Leonardos N. The bitcoin backbone protocol: Analysis and applications. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Berlin, Heidelberg: Springer; 2015:281–310.
19. Pass R, Tech C, Seeman L. *Analysis of the Blockchain Protocol in Asynchronous Networks*. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Cham, Switzerland: Springer; 2017:643–673.
20. Sompolinsky Y, Zohar A. Secure high-rate transaction processing in Bitcoin. *International Conference on Financial Cryptography and Data Security*. Springer; 2015:507–27.
21. Eyal I. The miner's dilemma. *2015 IEEE Symposium on Security and Privacy*. IEEE; 2015:89–103.
22. Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. *International Conference on Financial Cryptography and Data Security*. Springer; 2014:436–54.
23. Buterin V. *A Next-generation Smart Contract and Decentralized Application Platform*. https://github.com/ethereum/wiki/wiki/White-Paper. Accessed July 31, 2016.
24. Wood G. *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. http://www.cryptopapers.net/papers/ethereum-yellowpaper.pdf. Accessed October 11, 2016. 2014.
25. Ethereum Foundation. The Ethereum Project. https://www.ethereum.org/. Accessed December 16, 2016.
26. Ripple. The Ripple. https://ripple.com/. Accessed December 15, 2016.
27. Moreno-Sanchez P, Zafar MB, Kate A. Listening to whispers of ripple: Linking wallets and deanonymizing transactions in the ripple network. *Proc Privacy Enhancing Technol*. 2016;2016(4):436–53.
28. The Dash Network. The Dash Crypto Currency. https://www.dash.org/. Accessed April 13, 2017.
29. Duffield E, Diaz D. Dash: A Privacy-Centric Crypto-Currency. https://github.com/dashpay/dash/wiki/Whitepaper. Accessed April 13, 2017.
30. Litecoin Project. Litecoin - Open source P2P digital currency. https://litecoin.org/. Accessed December 15, 2016.
31. Stevenson J. *Getting started with Litecoins (after Bitcoin)*. John Stevenson; 2013. https://books.google.com/books?id=jk5zAgAAQBAJ. Accessed December 15, 2016.
32. The Monero Project. MONERO Private Digital Currency. https://getmonero.org/home. Accessed December 15, 2016.
33. Tarasiewicz M, Newman A. Cryptocurrencies as distributed community experiments In: Lee D, Kuo C. eds. *Handbook of Digital Currency*. Elsevier Inc; 2015:201–22.

34. Rosenfeld M. Overview of colored coins. https://bitcoil.co.il/BitcoinX.pdf. Accessed July 31, 2016.
35. Colored Coins. ColoredCoins Framework for digital currencies. http://coloredcoins.org/. Accessed December 15, 2016.
36. Back A, Corallo M, Dashjr L, *et al*. *Enabling Blockchain Innovations with Pegged Sidechains*. https://blockstream.com/sidechains.pdf. Accessed December 15, 2016.
37. Swan M. *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, Unitited States: O'Reilly Media, Inc.; 2015.
38. Bentov I, Lee C, Mizrahi A, Rosenfeld M. Proof of Activity: extending Bitcoin's Proof of Work via Proof of Stake [Extended Abstract] y. ACM SIGMETRICS. *Perform Eval Rev*. 2014;42(3):34–37.
39. King S, Nadal S. *Ppcoin: Peer-to-peer Crypto-currency with Proof-of-stake*. http://peerco.in/assets/paper/peercoin-paper.pdf. 2012. Accessed October 11, 2016.
40. Bentov I, Gabizon A, Mizrahi A. Cryptocurrencies without proof of work. *International Conference on Financial Cryptography and Data Security*. Berlin Heidelberg: Springer; 2016:142–157.
41. Bonneau J, Miller A, Clark J, Narayanan A, Kroll JA, Felten EW. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies. *2015 IEEE Symposium on Security and Privacy*. San Jose, California, United States: IEEE; 2015:104–21.
42. Bitcoin Wiki. Proof of burn. https://en.bitcoin.it/wiki/Proof_of_burn. Accessed October 11, 2016.
43. Intel Corporation. Hyperledger Sawtooth. https://intelledger.github.io/introduction.html. Accessed December 15, 2016.
44. Gervais A, Karame GO, Wuüst K, Glykantzis V, Ritzdorf H, Capkun S. *On the Security and Performance of Proof of Work Blockchains*. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. Vienna, Austria: ACM; 2016:3–16.
45. McConaghy T, Marques R, Müller A, *et al*. *BigchainDB: A Scalable Blockchain Database*. https://www.bigchaindb.com/whitepaper/. Accessed July 30, 2016.
46. Greenspan G. *MultiChain Private Blockchain*. http://www.multichain.com/download/MultiChain-White-Paper.pdf. Accessed July 30, 2016.
47. Vukolić M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. *International Workshop on Open Problems in Network Security*. Zurich, Switzerland: Springer; 2015:112–25.
48. Mainelli M, Smith M. Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology). *J Financial Perspect*. 2015;3(3):38–69.
49. MultiChain. MultiChain open platform for blockchain applications. http://www.multichain.com/. Accessed December 16, 2016.
50. BigchainDB GmbH. BigchainDB The scalable blockchain database. https://www.bigchaindb.com/. Accessed December 16, 2016.
51. Kosba A, Miller A, Shi E, Wen Z, Papamanthou C. *Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts*. 2016 IEEE Symposium on Security and Privacy (SP). San Jose, California, United States: IEEE; 2016:839–858.
52. Omohundro S. Cryptocurrencies, smart contracts, and artificial intelligence. *AI Matters*. 2014;1(2):19–21.
53. Swan M. Blockchain thinking: The brain as a dac (decentralized autonomous organization). *Texas Bitcoin Conference*. Austin, Texas, United States: Texas Bitcoin Association; 2015:27–29.
54. Swan M. Blockchain Temporality: Smart Contract Time Specifiability with Blocktime. *International Symposium on Rules and Rule Markup Languages for the Semantic Web*. Stony Brook, New York, United States: Springer International Publishing; 2016:184–96.
55. Szabo N. The idea of smart contracts. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html. Accessed October 11, 2016.
56. Watanabe H, Fujimura S, Nakadaira A, Miyazaki Y, Akutsu A, Kishigami J. Blockchain contract: Securing a blockchain applied to smart contracts. *2016 IEEE International Conference on Consumer Electronics (ICCE)*. Las Vegas, Nevada, United States: IEEE; 2016:467–68.
57. Del Castillo M. *Microsoft Doubles Down on Ethereum With New Blockchain Product*. CoinDesk. http://www.coindesk.com/microsoft-launching-new-ethereum-blockchain-product/. Accessed December 16, 2016.
58. Kalodner H, Carlsten M, Ellenbogen P, Bonneau J, Narayanan A. An empirical study of Namecoin and lessons for decentralized namespace design. Workshop on the Economics of Information Security. Delft University of Technology, Netherlands: WEIS; 2015.
59. Namecoin.org. The Namecoin. https://namecoin.org/. Accessed December 16, 2016.
60. Bartling S, Fecher B. Could Blockchain provide the technical fix to solve science's reproducibility crisis? LSE Impact of Social Sciences blog. http://blogs.lse.ac.uk/impactofsocialsciences/2016/07/21/could-block-chain-provide-the-technical-fix-to-solve-sciences-reproducibility-crisis/. Accessed December 16, 2016.
61. Winton R. Hollywood hospital pays $17,000 in bitcoin to hackers. *FBI Investigating*. Los Angeles Times. http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html Accessed December 16, 2016.
62. McCarthy J. *MedStar Attack Found to Be Ransomware, Hackers Demand Bitcoin*. Healthcare IT News. http://www.healthcareitnews.com/news/medstar-attack-found-be-ransomware-hackers-demand-bitcoin Accessed December 16, 2016.
63. Meunier S. *Blockchain Technology — a Very Special Kind of Distributed Database*. Medium. https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118. Accessed April 6, 2017.
64. Martin L. *Blockchain vs. Relational Database: Which is right for your Application*? TechBeacon. https://techbeacon.com/Blockchain-relational-database-which-right-for-your-application. Accessed April 6, 2017.
65. *ONC/NIST Use of Blockchain in Healthcare and Research Workshop*. 2016. https://oncprojectracking.healthit.gov/wiki/display/TechLabI/Use of+Blockchain+in+Healthcare+and+Research+Workshop. Accessed December 20, 2016.
66. Elmasri R, Navathe SB. *Fundamentals of Database Systems*. Boston, Massachusetts, United States: Pearson Education, Inc.; 2016.
67. Özsu MT, Valduriez P. *Principles of Distributed Database Systems*. New York, United States: Springer Science+Business Media; 2011.
68. Oracle. The Oracle Database. https://www.oracle.com/database/index.html. Accessed April 13, 2017.
69. The Apache Software Foundation. *Apache Cassandra*. http://cassandra.apache.org/. Accessed April 13, 2017.
70. Lorenz J-T, Münstermann B, Higginson M, Olesen PB, Bohlken N, Ricciardi V. *Blockchain in Insurance – Opportunity or Threat*? McKinsey & Company. http://www.mckinsey.com/~/media/McKinsey/Industries/Financial Services/Our Insights/Blockchain in insurance opportunity or threat/Blockchain-in-insurance-opportunity-or-threat.ashx. Accessed April 21, 2017.
71. *FIPS PUB 180-4 Secure Hash Standard (SHS)*. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf. Accessed April 6, 2017.
72. Bitcoin Wiki. SHA-256. https://en.bitcoin.it/wiki/SHA-256. Accessed April 6, 2017.
73. *FIPS PUB 186-4 Digital Signature Standard (DSS)*. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf. Accessed April 6, 2017.
74. Bitcoin Wiki. *Elliptic Curve Digital Signature Algorithm*. https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm. Accessed April 6, 2017.
75. Baxendale G. Can Blockchain Revolutionise EPRs? *ITNOW*. 2016;58(1):38–39.
76. Mettler M. Blockchain technology in healthcare: The revolution starts here. *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*. Munich, Germany: IEEE; 2016:1–3.
77. Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *J Med Syst*. 2016;40(10):218.
78. Blough D, Ahamad M, Liu L, Chopra P. MedVault: Ensuring security and privacy for electronic medical records. *NSF CyberTrust Principal*

Investigators Meeting. 2008. http://www.cs.yale.edu/cybertrust08/posters/posters/158 medvault poster CT08. pdf. Accessed December 20, 2016.
79. Snow P, Deery B, Kirby P, Johnston D. *Factom Ledger by Consensus: Retrieved from Factom*. 2015. http://www.factom.org. Accessed December 20, 2016.
80. Sarwal A, Insom P. BitHealth. https://devpost.com/software/bithealth. Accessed December 20, 2016.
81. Gem. Gem Health Network. https://gem.co/health/. Accessed December 20, 2016.
82. Yuan B, Lin W, McDonnell C. *Blockchains and Electronic Health Records*. http://mcdonnell.mit.edu/blockchain_ehr.pdf. Accessed October 11, 2016.
83. Witchey NJ. *Healthcare Transaction Validation Via Blockchain Proof-of-work, Systems and Methods*. United States patent application US 14/711,740; 2015.
84. Gropper A. Powering the Physician-Patient Relationship with HIE of One Blockchain Health IT. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
85. Ivan D. Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
86. Linn LA, Koo MB. Blockchain for health data and its potential use in health IT and health care related research. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
87. Prakash R. Adoption of blockchain to enable the scalability and adoption of accountable care. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
88. Krawiec R, Barr D, Killmeyer J, *et al*. Blockchain: opportunities for health care. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
89. C B, Kalis B, Mitchell E, Pupo E, Truscott A. Blockchain: securing a new health interoperability experience. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
90. Guardtime. Guardtime Industrial Blockchain. https://guardtime.com/. Accessed December 20, 2016.
91. Williams-Grut O. *Estonia is Using the Technology Behind Bitcoin to Secure 1 Million Health Records*. Business Insider Inc. http://www.businessinsider.com/guardtime-estonian-health-records-industrial-blockchain-bitcoin-2016-3. Accessed December 20, 2016.
92. Attili S, Ladwa SK, Sharma U, Trenkle AF. Blockchain: the chain of trust and its potential to transform healthcare – our point of view. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
93. Yip K. Blockchain & alternate payment models. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
94. Culver K. Blockchain Technologies: A whitepaper discussing how the claims process can be improved. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
95. Vian K, Voto A, Haynes-Sanstead K. A blockchain profile for medicaid applicants and recipients. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
96. 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*. Use of Blockchain for Healthcare and Research Workshop. 2016.
97. Azaria A, Ekblaw A, Vieira T, Lippman A. MedRec: using blockchain for medical data access and permission management. *International Conference on Open and Big Data (OBD)*. Vienna, Austria: IEEE; 2016:25–30.
98. Peterson K, Deeduvanu R, Kanjamala P, Boles K. A blockchain-based approach to health information exchange networks. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
99. McKernan KJ. The chloroplast genome hidden in plain sight, open access publishing and anti-fragile distributed data sources. *Mitochondrial DNA* Part A. 27(6):4518–4519.
100. Shrier AA, Chang A, Diakun-thibault N, *et al*. Blockchain and Health IT: Algorithms, Privacy, and Data. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
101. Goldwater J. The use of a blockchain to foster the development of patient-reported outcome measures. *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*. Gaithersburg, Maryland, United States: ONC/NIST; 2016.
102. Healthbank.coop. HealthBank. https://www.healthbank.coop/. Accessed December 20, 2016.
103. Nugent T, Upton D, Cimpoesu M. Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research* 2016;5: 2541.
104. Topol EJ. Money back guarantees for non-reproducible results? *BMJ*. 2016;353:i2770.
105. Taylor P. Applying blockchain technology to medicine traceability. SecuringIndustry.com. https://www.securingindustry.com/pharmaceuticals/applying-blockchain-technology-to-medicine-traceability/s40/a2766/ -.WFnPQ7GZNzg. Accessed December 20, 2016.
106. Jenkins J, Kopf J, Tran BQ, Frenchi C, Szu H. Bio-mining for biomarkers with a multi-resolution block chain. *SPIE Sensing Technology+ Applications: International Society for Optics and Photonics*. 2015; 9496:94960N.
107. HL7.org. Fast Healthcare Interoperability Resources (FHIR). https://www.hl7.org/fhir/. Accessed February 15, 2017.
108. Del Castillo M. *SWIFT: Blockchain Won't Remove All Third Parties in Securities Trade*. CoinDesk. http://www.coindesk.com/swift-research-blockchain-third-parties/. Accessed December 21, 2016.
109. De Filippi P. *The Interplay Between Decentralization and Privacy: the Case of Blockchain Technologies* 2016; 9.
110. Moser M. *Anonymity of Bitcoin Transactions*. Münster Bitcoin Conference. Münster, Germany: MBC; 2013:17–18.
111. Biryukov A, Khovratovich D, Pustogarov I. Deanonymisation of clients in Bitcoin P2P network. *2014 ACM SIGSAC Conference on Computer and Communications Security*. Scottsdale, Arizona, United States: ACM; 2014.
112. Ludwin A. *How Anonymous is Bitcoin*? Coin Center. https://coincenter.org/entry/how-anonymous-is-bitcoin. Accessed April 6, 2017.
113. Abbas A. *Understanding Privacy: How Anonymous can Bitcoin Payments be*? Bitcoinist.net. http://bitcoinist.com/understanding-privacy-anonymous-bitcoin/. Accessed April 6, 2017.
114. Blockchain Luxembourg S.A. *Confirmed Transactions Per Day*. https://blockchain.info/charts/n-transactions. Accessed December 14, 2016.
115. Visa Inc. *Visa Acceptance for Retailers*. https://usa.visa.com/run-your-business/small-business-tools/retail.html. Accessed December 14, 2016.
116. Meiklejohn S, Pomarole M, Jordan G, Levchenko K, McCoy D, Voelker GM, Savage S. A fistful of bitcoins: characterizing payments among men with no names. *2013 Internet Measurement Conference*. Barcelona, Spain: ACM; 2013:127–140.
117. Decentralizing privacy: using blockchain to protect personal data. *2015 IEEE Symposium on Security and Privacy Workshops*. San Jose, California, United States: IEEE; 2015:180–184.
118. Kish LJ, Topol EJ. Unpatients [mdash] why patients should own their medical data. *Nat Biotechnol*. 2015;33(9):921–24.
119. Kiayias A, Panagiotakos G. Speed-security tradeoffs in blockchain protocols. *IACR Cryptology ePrint Archive*. 2015;2015:1019.
120. Ohno-Machado L, Bafna V, Boxwala AA, *et al*. iDASH. Integrating data for analysis, anonymization, and sharing. *J Am Med Inform Assoc*. 2012;19:196–201.
121. Ohno-Machado L. To share or not to share: that is not the question. *Sci Transl Med*. 2012;4(165):165cm15.