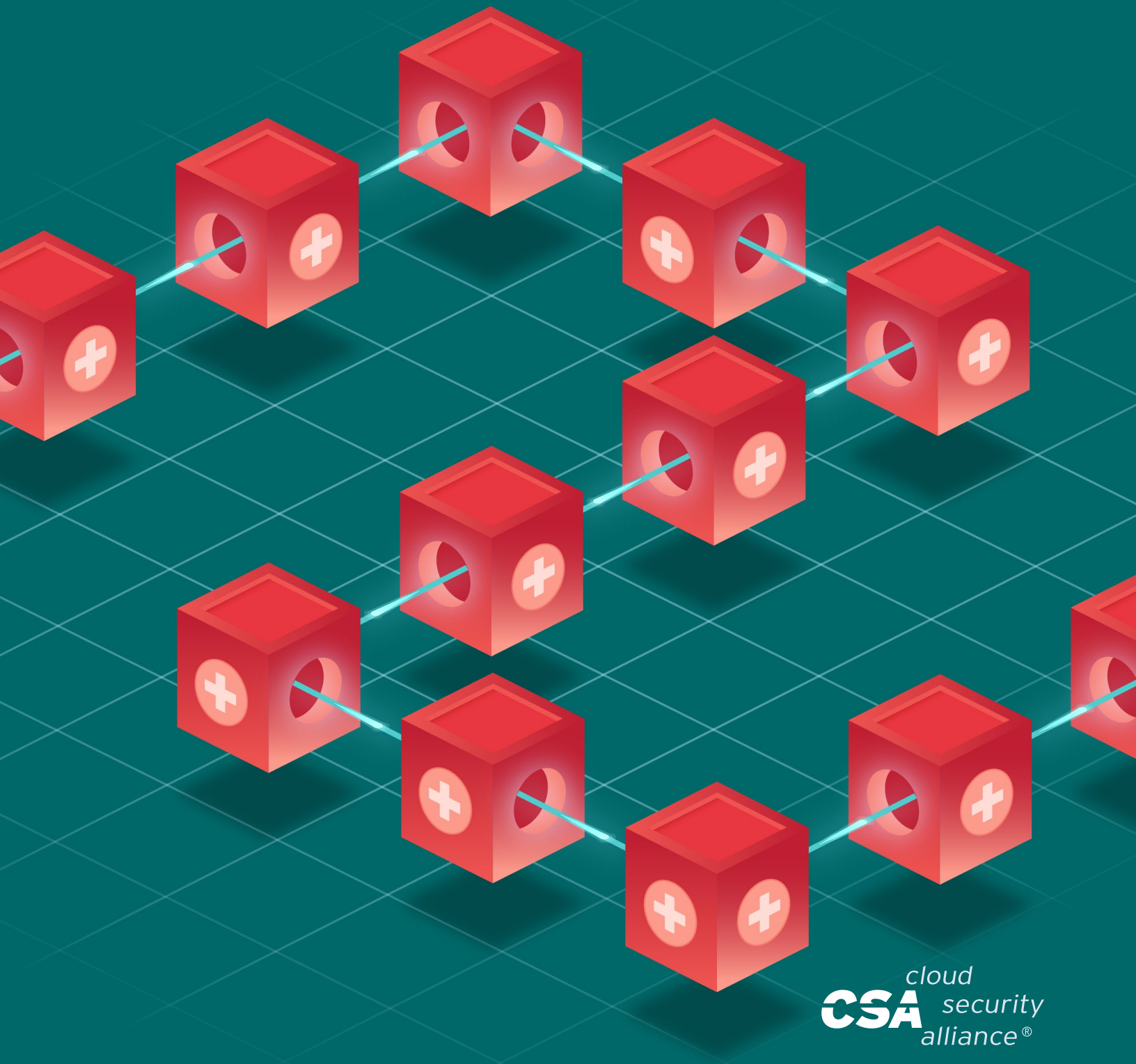
The Use of Blockchain in Healthcare



cloud security alliance®

The permanent and official location for the Health Information Management Working Group research is:
https://cloudsecurityalliance.org/research/working-groups/health-information-management/

Acknowledgments

Lead Authors:

Dr. James Angle

Contributors:

Rea Achalkar
Danielle Cadoret
Ken Huang
Ciju John
Gurpreet Singh Maini
Ashish Mehta
Alexandre Caramelo Pinto
Michael Roza
Adalberto Valle

CSA Global Staff:

Hillary Baron
Vince Campitelli
Alex Kaluza
AnnMarie Ulskey (Design)

The CSA's Health Information Management Working Group aims to directly influence how health information service providers deliver secure cloud solutions (services, transport, applications, and storage) to their clients and foster cloud awareness within all aspects of healthcare and related industries. The working group research will continue to be freely available for use without license fees or restrictions by the CSA.

Table of Contents

Abstract

The unique attributes of Healthcare data's unique attributes make it a prime target for nefarious actors. Predictably, healthcare information is tightly regulated by privacy and security laws in the United States and European Union and international rules governing cloud data storage. The data's high value—coupled with these regulatory requirements—has motivated organizations to explore using blockchain to secure data. Blockchain is a digital ledger consisting of a "chain of blocks." Transactions added to a new block are validated before inclusion in the block. When the block is completed, it is appended in chronological order to the end of an existing chain of blocks. Blockchain is unique because there are only two possible transactions: "add transaction" and "view transaction." Transactions can never be deleted or edited. This limited set of actions helps ensure data integrity—a critical element for healthcare, as well as non-repudiation. Ultimately, blockchain may enable efficient healthcare data sharing while ensuring patient privacy and data security.

Introduction

The healthcare industry is vast and heavily regulated. In the U.S. healthcare privacy and security issues are primarily regulated by the Health Insurance Portability and Accountability Act (HIPAA). In the EU, the General Data Protection Regulation (GDPR) is the central privacy and security regulatory driver. Both HIPAA and the GDPR require healthcare organizations to protect personal and health information, and each regulatory body can levy fines for data breaches. In the U.S. Healthcare Delivery Organizations (HDO) are encouraged to implement Electronic Health Records (EHR) under the Affordable Care Act (ACA). This initiative's goal is to provide healthcare professionals with patient record access "anywhere, anytime." In response, states have created cloud-based health information exchanges to collect and share patient information. Health record storage and accessibility considerations present privacy and security concerns. As these cloud-based storage systems add more health records, they become even more attractive hacking targets. The COVID-19[1] pandemic has hastened the creation, storage, and transmission of large amounts of electronic protected health information (ePHI) with the rapidly growing use of telehealth. This industry trajectory has placed a spotlight on data protection.

Data security concerns are valid: in 2018, 15 million patient records were compromised in 503 breaches—three times the amount seen in 2017 (Davis, 2019). The loss of Personally Identifiable Information (PII) occurs it can hurt the reputation of the organization, financial loss, an increased risk of further identity theft and data compromise, and exposure to lawsuits. The ramifications of an HDO data breach can be serious, given the sensitive nature of the data they store (Osborne, 2020).

The 2020 Verizon Data Breach Investigations Report (DBIR) reported 798 data breach incidents globally; 521 cases—or 65 percent—of this total were confirmed as healthcare-related data disclosures. Amongst these reported healthcare breaches, 77 percent were related to PII, and 67 percent were medical data in nature. Healthcare data breaches are now common in news headlines, which is a growing concern.

[1] COVID-19 is a disease caused by a new strain of coronavirus. 'CO' stands for corona, 'VI' for virus, and 'D' for disease. Formerly, this disease was referred to as '2019 novel coronavirus' or '2019-nCoV.'

Blockchain technology can transform health care, place the patient at the center of the healthcare ecosystem, and increase privacy and security. This highly-touted approach—called "patient-centric healthcare"—empowers patients to control their healthcare and leads to better outcomes and greater patient satisfaction (Epstein et al., 2011). Blockchain may also provide a new model for health information exchanges (HIE) by making electronic medical records management more efficient and secure. The increased use of blockchain technology as a responsible and transparent mechanism to store and distribute data provides new potential to solve serious data privacy, security, and integrity issues in healthcare (Khezr et al., 2019).

Decentralization	• Electronic health records are stored, accessed, and managed at multiple locations. • Network is control by many entities. • Consensus protocols govern the network.
Immutability	• EHR and PHR of patients cannot be changed. • Asymmetric key cryptography and consensus protocols ensure the immutability of medical health records.
Transparency	• The transparency facilitates remote patient centered data control to share and enquire about any suspicious activities by information users.
Open Source Access	• Patients can access a physician's profile before scheduling an appointment for remote consultancy • The medical records are protected to assure regularity compliance operations
Auditability	• Drug administrative authorities can trace thl provenance of a drug. • The medical records are protected to assure regularity compliance operations.
Anonymity	• Anonymous identities of Telemedicine partici-pants. • Data and transactions are secured.

Figure 1: An overview of key elements and features of blockchain technology for telehealth and telemedicine.[2]

Healthcare technology advances are typically driven by needs for patient care improvements, demands for more accurate medical data analysis, and calls for easier, faster access to healthcare data (Panner, 2019). Blockchain technology will enhance patient information privacy and security concerns, and data integrity (as examined in this document). Blockchain technology will be described, as will different use cases for blockchain in healthcare. Finally, the paper will explore the current healthcare ecosystem, the potential use of blockchain technology-based solutions in the industry, and a presentation of several use cases.

[2] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7842132/

Blockchain

Recording transactions in a distributed, secure form that prevents modification and repudiation (when the transaction originator later claims they did not perform the action) is called Distributed Ledger Technology (DLT). An inherent feature of DLTs is that multiple replicas of the list of transactions exist, making it extremely difficult (if not impossible) to tamper with information.

Blockchain, the best-known DLT (but not the only one), is the technology behind Bitcoin. With Bitcoin's release, cryptocurrencies became the first use case of the blockchain. Recently, there has been increased awareness that blockchain has much more to offer than cryptocurrencies, as the technology can be an ideal tool for creating trust-based solutions.

Blockchain is a database consisting of a physical, fixed-length of blocks that includes "1 to N" transactions. Each transaction added to the block is validated before it is included in the block. When completed, the block is added to the end of the chain of blocks. Blockchain is an open distributed database, meaning that anyone provided with the requisite credentials can access and add to the ledger (Bambara et al., 2018). Data are added chronologically to the blockchain, and each block contains relevant, encrypted data—referred to as a hash—and the hash of a previous block. Only two operations can be performed—"add transaction" and "view transaction"—making blockchain ideal for various medical applications.

Blockchain is a peer-to-peer, distributed, append-only database of immutable and tamper-proof records. Each blockchain has a set of rules that determine whether a block created is valid or not, and only valid blocks are added to the chain. This set of rules form the basis of consensus in the blockchain. Consensus is the mechanism for agreeing to a common version of the blockchain with the "trusted truth," which means that transactions are created, authenticated, then added in a certain way (Katuwal et al., 2018).

With increased blockchain understanding and use, its utility has expanded beyond currency (such as Bitcoin) and migrated to concepts such as identity and property rights. As with other technologies, such as cloud computing, different blockchain deployment models have emerged.

- In a public blockchain model, anyone can participate in the consensus process and validate transactions. Transactions are public, and the blockchain is maintained by the public community (blockchain network participants), so there is the highest level of decentralized trust. In a public blockchain, no single user is trusted to verify transactions. All users follow an algorithm that verifies transactions.
- In a federated or consortium blockchain (a distributed ledger), a predefined set of consortium nodes with prescribed roles controls the consensus process. The right to read the ledger may or may not be public.
- In a private blockchain, write permissions are restricted to one centralized governing organization. Transactions are validated internally and may or may not be publicly readable. A private blockchain can provide a solution for compliance with HIPAA.

Smart Contracts

One highly appealing blockchain application for healthcare is the smart contract feature. A smart contract is a self-enforcing agreement embedded in code. The contract has a set of agreed-upon rules. When rules are met, agreements are enforced. Smart contracts allow for insurance claim payments and are also usable as gateways to store standardized information (which can be immediately accessible). Smart contracts require HDOs to enter information and, upon data entry completion, contracts are enforced, and claims are submitted. Values are stored on a blockchain and protected from tampering and revision, and cannot be deleted. Smart contracts, therefore, provide a transparent, verifiable way to embed auditable and enforceable governance rules and business logic in a code.

General

Blockchain has tremendous healthcare industry value in areas of:

1. research
2. supply chains
3. finance
4. facility and energy management
5. telehealth
6. patient administration.

Blockchain provides two critical, advantageous elements for healthcare use. The first is verifiability. Blockchain validates transactions, which provides HDOs with confidence and trust in information accuracy. The second is traceability. Because the information contained in a block cannot be changed and data is entered chronologically, it provides a traceable transactions record and assures the block has not been inappropriately modified. This data immutability and traceability is a critical requirement for HDOs. While verifiability and traceability are essential, one other process is required to ensure confidentiality: all healthcare information should be encrypted with strong encryption protocol end to end during data processing, storage, or transmission (Katuwal et al., 2018).

Research

Blockchain technology can provide solutions for data provenance, integrity, and security in research projects. Healthcare delivery organizations spend extensive time and money searching for clinical trial candidates. Therefore, it is vital to identify and recruit the best candidates quickly. Despite considerable advancements in digital recordkeeping, HDOs still navigate challenging issues regarding the sharing of patient data across provider and organizational networks. Many providers and organizations do not trust each other enough to share information on each others' platforms, as they are ultimately liable for patient record breaches. This mistrust has caused profound interoperability and data sharing issues translating to dire implications for inter-organizational patient treatment and limitations on conducting clinical research, which requires real-life medical data. Due to its decentralized and immutable properties, blockchain offers a possible solution to data sharing and/or access issues with full traceability of

assignment without prejudice to intellectual property (IP) rights. Organizations can join blockchains without central governing bodies, allowing entities that do not trust each other to interact and freely share data in an authorized manner.

Healthcare delivery organizations must capture clinical data to inform operations. Enabling practitioners with access to relevant clinical data—such as information regarding diagnosis, therapeutic planning, and direct patient treatment and care—is a basic operational need. Blockchain databases have trust built-in (with a degree of transparency). Shared ledgers can facilitate information sharing in a clinical study using cryptography. This platform type is vital in helping researchers and practitioners get direct and secure access to a vast repository of accurate clinical data (Shah & Kondaka, 2018).

Attaining more accurate clinical research outputs depends on the availability of large data sets of de-identified raw data from actual patients. Robust inter-organizational health information exchange enables access to patient clinical data across multiple HDOs. While blockchain technology alone may not fix patient identification issues, it can help enhance data integrity, accessibility, security, privacy, and interoperability.

Clinical trials using blockchain realize many benefits. Blockchain provides an immutable ledger for every research project step, and research participants can access all the data (which is time-stamped). Furthermore, the data is tamper-proof since all additions must be agreed upon by a majority of the network nodes before the record is accepted.

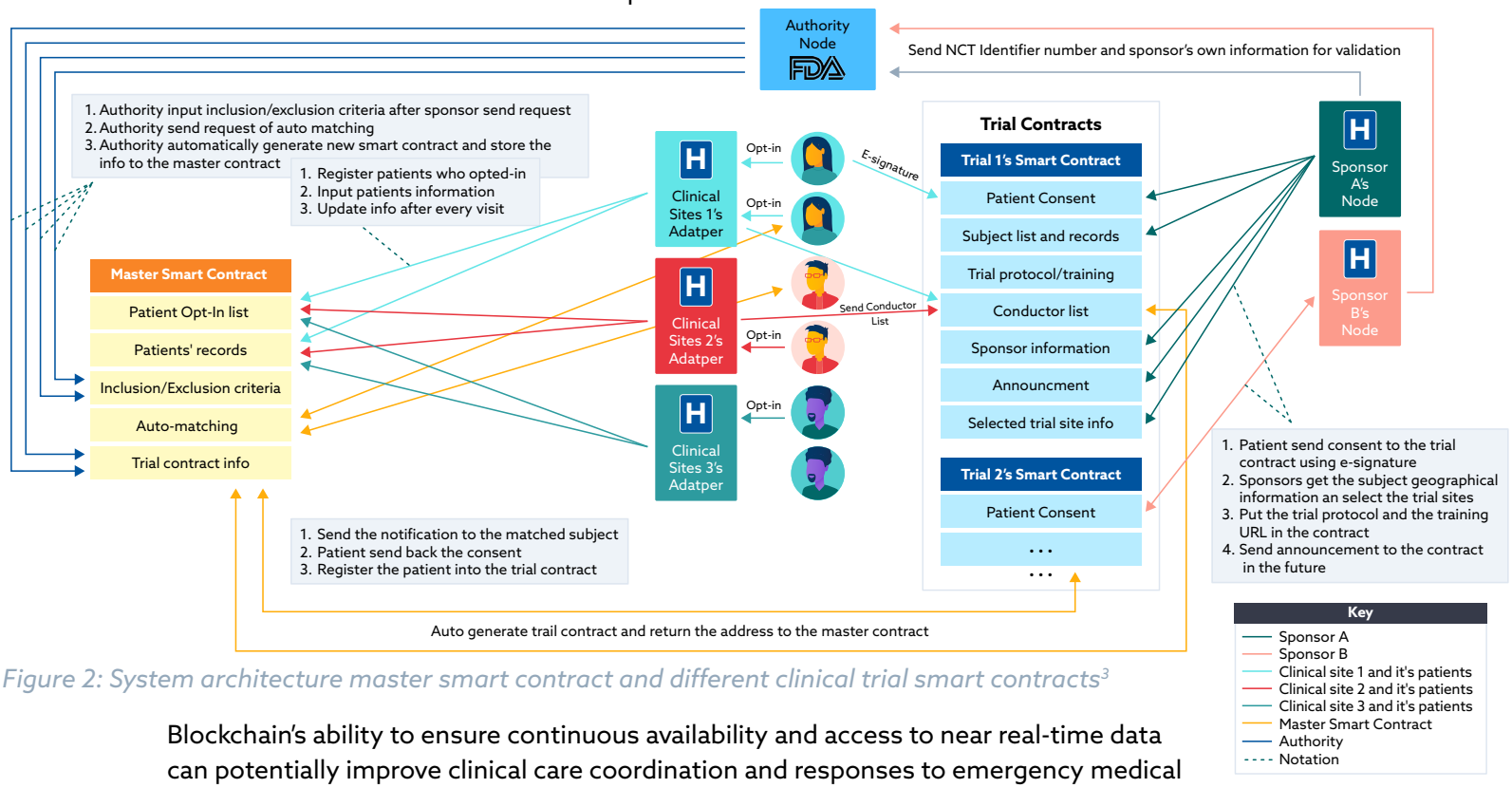


Figure 2: System architecture master smart contract and different clinical trial smart contracts[3]

Blockchain's ability to ensure continuous availability and access to near real-time data can potentially improve clinical care coordination and responses to emergency medical situations, such as COVID-19. Near real-time access may also allow researchers and public health resources to rapidly detect, isolate and drive change for environmental conditions that impact public

[3] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7153067/

health. Since blockchains enable continuous availability and access to historical data, researchers can easily extrapolate data and make predictive analyses based on previously stored blockchain data records.

Blockchain-based prototypes for electronic health records and medical research data utilize crucial properties of provenance. Distributed blockchain solutions address verification requirements, and records are signed to verify legitimacy and illegitimacy.

Additionally, blockchain provides privacy and security to the research project. At any point, research participants can add consent with confidence that data will be handled securely (Tsung-Ting et al., 2017).

Supply Chain

Medical supply chains must be managed in ways that provide traceability. Blockchain offers solutions for maintaining information in open, safe, and tamper-proof systems accessible to multiple parties. Blockchain technology using smart contracts could innovate healthcare contract management by providing real-time contract tracking and execution while allowing users to determine if contracts have been completed satisfactorily (Stagnaro, 2017). Blockchain in healthcare may automate supplier contracts and apply analytics on a wide range of metadata regarding goods and services. Results could increase productivity, reduce costs and improve quality control.

Blockchain is uniquely situated as a monitoring technology for the whole medical supply movement process. All blockchain transactions are recorded into the ledger, and every node in the blockchain maintains a complete transactions record, making it easy to verify supply origins, vendors, and distributors.

Important examples of this concept include vaccine and medication supply chains. The global market for counterfeit medicines accounts for nearly U.S. $200 billion per year, and consumption of fraudulent products significantly impacts health outcomes (U.S. Department of Commerce, 2016). Replacing current supply chain management technologies with blockchain can flesh out chain vulnerabilities, significantly reduce corruption opportunities by chain stakeholders, and verify every product exposure location and contact. Furthermore, regulatory body inclusion in the blockchain enhances product legitimacy and trust via greater oversight.

Through increased supply chain insight and accurate, timely reporting, HDOs can ensure supplies reach high-needs patients. Blockchain technology also provides a significant improvement to demand forecasting and data provenance processes.

Financial

Blockchain can transform the financial services industry through faster throughput, reduced costs, fewer errors, and transparency (Bambara et al., 2018). Smart contracts amplify these benefits. Smart contract structures allow nodes to execute contract transactions. This logic ensures accurate completion of claims and supports compliance audits using business rules. Supply chain billing and medical claims billing can use this process. Medical payers are encouraging HDOs to adopt

digital payment systems that offer high-level interoperability, faster payment processing, and safer electronic data interchange processing.

Billing Processing

Blockchain has shown promise in the medical billing industry. Medical billing processes are integral parts of healthcare and involve several steps: patient check-in, coding and billing compliance, claims transmission, and finally, insurance company compensation (Arsene, 2020). The whole billing process can be challenging, as payments may come from multiple health insurance providers and patients. Blockchain platforms can be built and implemented to quickly and accurately process claims. Smart contracts ensure that required information is entered before submitting claims, reducing processing time. Smart contracts also provide real-time transparency to patients and providers about claims status so claims can be finalized in real-time. Reduced processing times may result in increased efficiency and reduced expenses that allow HDOs and insurers to manage claims transparently, quickly, and in an indisputable manner.

Billing and Medical Coding

Medical care administrators—such as practice management companies or hospital staff—navigate complex medical coding levels. Serious potential pitfalls include unintentional billing mistakes (such as duplicating processes or incorrect filings) resulting in denied claims. For patients, denied claims may result in unrecoverable financial losses, while companies may realize massive financial burdens.

Additionally, patients and healthcare providers may also perpetrate willful inaccuracies (classified as fraud). Blockchain inherently uncovers fraud—whether intentional or otherwise—via transparency and provenance. This functionality allows stakeholders (such as insurance companies) to authenticate every patient encounter, verify diagnoses (with International Classification of Diseases (ICD) codes), and identify erroneous transactions (through careful audit using smart contracts, which evaluates treatments, medicines, causes, and effects).

Coding and billing inaccuracies (including medical fraud) can compromise patient care, generate revenue loss, and lead to severe consequences, such as hefty government penalties and fines.

Facility and Energy Management

The healthcare sector's use of blockchain technology for facility and energy management is vital. From vendor/supplier smart contract creation to automation through self-executing capabilities, every detail and process is trackable through digital contracts. Permanent, auditable digital records empower stakeholders to trust performance levels, ensure compliance issues are closed out, and authenticate that financial aspects are automatically addressed on completion of scope.

From an energy management perspective, utility and facility management cost reductions directly impact health care development profitability. Automation systems must adapt to actual usage requirements considering the infrastructure necessary for Heating, Ventilation, and Air Conditioning

(HVAC), plumbing, lighting, power, medical gas, and other systems. This enhancement is possible only through relevant data collection on the various building profiles (e.g., occupancy, outdoor conditions, lighting requirements, or additional building occupant needs). Blockchain technology allows real-time data management and authentication across all equipment. Based on advanced Business Management System (BMS)/Building Automation System (BAS) algorithms and Proportional-Integral-Derivative (PID) control loops, there is an opportunity to automate equipment energy optimization within buildings while continuously monitoring maintenance requirements to ensure appropriate, timely action when needed.

Telehealth

Telehealth is more than just video conferencing. The practice encompasses four modalities.

1. Mobile health: This includes smartphone and tablet application data collection.
2. Remote patient monitoring: This includes gathering patient data from medical devices and wearable devices (such as fitness monitors) classified as the Internet of Medical Things (IoMT).
3. Store and forward: In this scenario, data (such as radiology and laboratory results) are stored for download by medical personnel later.
4. Videoconferencing: A one-to-one, real-time session between a medical provider and a patient.

Telehealth demand has increased dramatically since the COVID-19 pandemic started. This worldwide health emergency led to several waivers from the U.S. Department of Health and Human Services and the Office for Civil Rights (OCR)—which oversee HIPAA—to facilitate remote care data sharing while lowering viral exposure risks for HDOs and patients.

While convenient, telehealth technology raises security concerns. If either end of the virtual connection is unsecured, sensitive patient information could be leaked (Siwicki, 2019). Telehealth can benefit from blockchain technology by introducing a trust layer between patients and healthcare professionals. Blockchain-based telehealth platforms can validate professional identity, provide data integrity, and ensure transparency and traceability.

Suppose doctor-patient relationships and sensitive information cannot be protected during telehealth interactions. Will the practice ever gain widespread support from patients, healthcare providers, and—most importantly—the OCR? Blockchain helps establish seamless, secure data exchange between providers and patients in telehealth settings. With blockchain, patients and medical professionals must approve all data entered into the computer and verify information against a previous ledger. Both patients and doctors secure a ledger copy to enable multiple checks for protecting sensitive data (Wabo, 2019).

The IoMT is a growing domain within Internet of Things (IoT) applications where devices provide different healthcare services. Typically, IoMT devices are attached to the body and collect data, enabling HDOs to make timely, data-driven decisions. The IoMT devices pose major security and privacy challenges and tend to be resource-constrained (meaning they have insufficient memory and processing powers for traditional security algorithms). Additionally, centralization used in state-of-the-art security frameworks is not well-suited for IoMT devices (Seliem et al., 2019).

Patients are the data sources for IoMT devices, which develop significant volumes of data. The generated information is stored on blocks and often in the cloud. Artificial intelligence (AI) can help blockchains create intelligent virtual agents to produce new ledgers automatically (Khezr et al., 2019).

Because IoMT devices play a vital role in telehealth information systems, they can benefit from blockchain integration. Using cloud computing, IoMT technology (such as heart monitors, body scanners, and wearable health devices) can gather, process, and share data in real-time. Blockchain's decentralized, distributed, and public digital ledger can store data across its peer-to-peer network, and the technology eliminates data centralization risks, such as data manipulation. Based on its architecture, blockchain is a sound choice for IoMT device security and privacy.

Patient Administration

Until recently, medical records were paper-based, and a patient could have multiple records if interacting with numerous providers and specialists. This environment made it difficult to monitor a patient's health status. In the U.S. the American Recovery and Reinvestment Act required all public and private health care providers to adopt electronic medical records (EMR) by Jan. 1, 2014, to maintain their existing Medicaid and Medicare reimbursement levels. This mandate incentivized HDOs to adopt electronic health records (EHR). Healthcare providers with EHR access significantly improved patient care and reduced errors. Additionally, EHR provided a data source for big data analytics, enabling better care management and preventive care.

Advances in health-related data collection, cloud storage, and privacy protection laws— coupled with data viewing and sharing needs—provide new opportunities and challenges in health data management. While privacy protection laws make it more complicated to share patient information (even in critical situations) freely, blockchain provides increased data control and access for individual patients. Blockchain pushes electronic health data toward patient-centric healthcare and potentially allows patients (not HDOs) to oversee their medical records. With blockchain, medical records travel with patients, who can choose to give (or revoke) consent to healthcare practitioners regarding records access. Ensuring data security in all stages of the data life cycle and managing data use, access, and integration are crucial considerations for data-driven organizations, such as healthcare providers.

While EHR systems can help facilitate patient information sharing throughout the same hospital system, merging patient data scattered across multiple EHRs poses a challenge. For example, electronic health records may belong to different HDOs who do not have a data-sharing agreement established. Interoperability issues may also hamper access, especially when HDOs use incompatible EHR software that cannot communicate. Blockchain technology can help deliver solutions efficiently and effectively in response to these issues (Khezr et al., 2019). Furthermore, blockchain can address interoperability issues in healthcare information technology (IT) systems, evolving into the technical standard that enables individuals, HDOs, and medical researchers to securely share electronic health data (Linn et al., 2016). Sophisticated application programming interface (APIs) can ensure EHR interoperability and data storage is a reliable process.

Security Issues

Blockchain technology alone does not eliminate cybersecurity risks, and the structure is subject to many of the same threats and vulnerabilities as other technologies. A robust cybersecurity program remains vital to protecting the network from cyber threats. Healthcare delivery organizations must still rely on current standards and guidelines to ensure blockchain technology systems' security. This mandate is particularly true regarding cloud security, as data storage security is a critical aspect of blockchain security.

Blockchain technology is considered secure in that it is tamper-resistant once a transaction is completed. However, it may be vulnerable to attack before it is included in the published block. Blockchain might also be susceptible to time spoofing, which could affect the order of the transactions or denial-of-service attacks on smart contracts. Furthermore, newly coded smart contracts could contain unknown vulnerabilities for later exploitation (Yaga et al., 2018).

Key management is another aspect of blockchain security. Some blockchains provide an online Key Management Service (KMS), allowing users to interact with the blockchain via traditional Representational State Transfer (REST), such as an API. Application programming interfaces are ideal from a security perspective, as they provide myriad security options that are well-studied. However, the KMS model also represents a single point of failure. This characteristic is not necessarily harmful if the KMS's central role is recognized and the service is adequately secured.

A more mainstream approach is to have users manage their keys. This is a more secure solution as it decentralizes the key management problem. The negative of this strategy is increased complexity and security vulnerability at the user end. User key security is prone to similar security vulnerabilities that plague password security, such as weak wallet security, social engineering attacks, software vulnerabilities, etc.

Security is about managing risk. Therefore, to use blockchain, it is critical to understand its threats and vulnerabilities. Blockchain security risks depend on blockchain types. For example, public blockchains allow anyone to join, making them riskier. Conversely, private blockchains restrict membership and are comparatively less risky. Permissionless blockchains have no restrictions on processes, while permissioned blockchains allow for ledger encryption so only participants can view it.

A well-constructed and secure healthcare blockchain implementation must incorporate several core properties of decentralization with a robust failover model allowing many participating system entities to avoid a single point of failure. Medical records should be stored locally in separate provider and patient databases, with authorization data copies stored on each network node. To ensure the system does not create a central target for content attack—a crucial consideration in an age of cyberattacks and data leaks—raw medical data and global authorization logs should be distributed.

There are several other blockchain risks, categorized broadly in three areas:

- **Business and governance:** Business risks include financial, reputational, and compliance concerns. Governance risks derive from the decentralized nature of blockchains and require strong controls, governing policies, identity, and access management.

- **Process:** These risks are associated with the processes a blockchain solution requires in its architecture and operations.
- **Technology:** The technology used to implement processes and business needs may not always be the best choice, and this can ultimately lead to security risks. (Arunkumar et al., 2019).

Securing Blockchain

A vital part of securing blockchain relates to personal keys used in encryption. Attackers can attempt to access personal keys stored in user computers or smartphones to hack the blockchain. Strong wallet authentication is strongly recommended to protect personal key storage, while Multi-Factor Authentication (MFA) should be used due to healthcare data sensitivity. Additionally, attackers can install malware on computers or smartphones to leak personal keys to hack the blockchain. Using hardware tokens for transaction approvals can protect personal keys against these attacks (Park et al., 2017).

Multi-party computation solutions (to sign transactions in a distributed fashion) were recently developed to secure user keys. These allow private keys to be split and distributed to disparate authorities, all of which must collaborate to sign individual transactions. Among additional advantages compared to other key management solutions, this action removes private keys as the single point of failure (Archer et al., 2018).

With increased blockchain use, malware and malicious code incidents targeting blockchain have also increased. Malware tools can be used to target a user's desktop and server and attack blockchain. Therefore, endpoint security is critical for detection and protection from malicious code.

The following steps should be implemented to secure the blockchain:

- Enforce identity and access controls to access blockchain solutions and data. Organizations using in-house Identity Access Management (IAM) systems should appropriate tokens such as OAuth, OpenID Connect, and Security Assertion Markup Language 2.0 (SAML 2.0) to authenticate, verify, and authorize functions. Additionally, organizations should limit privileged access and aggressively manage accounts to ensure policy compliance while mandating MFA to access the blockchain (with no exceptions).
- As with any cloud solution, APIs can be an issue. Application programming interfaces are the primary communication vehicle between the blockchain's different segments. Use API security best practices to safeguard API-based transactions, as API functionality must be protected from improper use and limited to the scope of the transaction.
- Ensure all platform communication between internal and external components interact through highly secure channels using mutual or standard Transport Layer Security (TLS). The TLS solution should be version 1.2 or higher.
- Use vigorous, reliable key management solutions to manage the number of blockchain keys, including blockchain identity keys, internal TLS certificates, external TLS certificates, and domain certificates. Encryption should be Federal Information Processing Systems (FIPS) 140-2 or higher.
- Perform testing at every phase of the organization's blockchain solution deployment and vulnerability assessments at the individual component level (and for the overall system) to ensure all issues are addressed. Also, perform penetration testing on the entire system (Arunkumar et al., 2019).

Blockchain technology requires organizational controls to ensure compliance with policies and regulations (such as HIPAA) and does not allow organizations to opt out of these responsibilities. Secure organizational infrastructure with recognized control frameworks, such as the National Institute of Standards and Technology (NIST) Risk Management Framework and NIST Cybersecurity Framework.

To ensure security, HIPAA requires HDOs to conduct risk assessments that include cloud computing threats. These assessments provide essential information for making risk-based telehealth decisions. Additionally, HDOs should identify all controls in place and ensure they are working as intended. Be mindful that security is a shared responsibility and, in most cases, HDOs can only assess internal controls. Healthcare delivery organizations must rely on third-party assessments of the service provider's security controls. This third-party attestation can include a SOC 2[4] Type 2 report or HITRUST[5] certification. Additionally, service providers may be certified by FEDRAMP[6] or the STAR registry. Lastly, the Cloud Security Alliance Security Trust & Assurance Registry[7] (CSA STAR) is a registry of certified cloud providers who have met the security requirements.

Blockchain in Healthcare Cases

Combat COVID-19 with Blockchain in China

The Chinese government prioritized blockchain integration in October 2019, when President Xi Jinping declared it an essential breakthrough technology for the country. The digital ledgers were already in use before the pandemic. China has filed among the highest numbers of blockchain patents in the world, with many Chinese startups and tech leaders (such as Baidu, Tencent, and Alibaba, or "BAT") working on real-world blockchain applications (including healthcare). In response to the pandemic, China has accelerated blockchain adoption and use for COVID-19 management. Since January 2020, Chinese hospitals with COVID-19 patients have utilized blockchain technologies in numerous capacities, ranging from electronic healthcare records and drug tracking to insurance claims. One blockchain application is the so-called "Health QR Code," which indicates via smartphone whether citizens are potentially contagious with COVID-19 and restricts citizen movement and access to public spaces. The Chinese government credits this technology in curbing infection rates.

Nearly every eligible Chinese citizen utilizes these codes, except Hong Kong and Macao residents. According to a recent People's Think Tank survey conducted online and through WeChat public forums, more than 90 percent of the 5,928 respondents applied for the code.

Although blockchain was effectively used to combat COVID-19 in China and the government moved quickly to publish required standards for data sharing, other issues—such as data privacy, consent management, and data security—are still in the early development stages. Leveraging decentralized identity standards (such as W3C DID) and cryptography (such as zero-knowledge proof, secure multiparty computing, threshold signatures, and homomorphic encryption) will be vital to protect citizen privacy.

[4] https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html
[5] https://hitrustalliance.net/
[6] https://www.fedramp.gov/
[7] https://cloudsecurityalliance.org/star/registry/

China BAT Blockchain for Healthcare

The three Chinese tech titans (BAT) have worked independently over the last three years on blockchain-based solutions to boost the country's medical infrastructure efficiency while keeping patient data secure.[8]

Baidu's Blockchain for Healthcare

Baidu—China's biggest search engine provider—launched a blockchain medical solution in September 2019 to securely distribute and share medical data. The open-source platform, called XuperChain, stores data relating to health records, diagnoses, treatments, and prescriptions. XuperChain is currently a regional pilot program that will eventually function as a national medical data depository with the capacity to facilitate insurance claims processing. In collaboration with the local government, this innovative blockchain solution, initially launched in Chongqing's Yuzhong District, is set to roll out nationwide over the next few years.[9]

In January 2020, Baidu launched a public beta for Xuperchain. Through blockchain, Baidu hopes to tackle the healthcare system's inefficiencies and high expenses—an estimated RMB 10 trillion ($1.4 trillion) in 2020. Initially, the project will focus on e-prescriptions to address communication shortfalls between hospitals and pharmacies. Both parties currently rely on different systems, which can result in lengthy patient waiting times. Baidu's blockchain will record the medical provider's initial prescription and drug delivery and collection information, streamlining the patient experience so doctors can fulfill e-prescriptions remotely with pharmacies.

Trust in Baidu's blockchain program will be dependent on the company's official partners, which host the blockchain's nodes. These stakeholders include the Beijing and Guangzhou Internet Courts, the Arbitration Commission, and the Copyright Bureau. Baidu also offers its blockchain as a service (BaaS) platform and the Baidu Blockchain Engine (BBE). The BBE supports Ethereum, Hyperledger Fabric, and Solidity smart contracts.

The Baidu Blockchain Engine has been applied to the transport of hazardous chemicals by tracking and sharing heavy goods vehicle information such as the vehicle routes and speeds.[10]

Alibaba's Blockchain for Healthcare

Alibaba launched its medical application blockchain in 2017. Additionally, the e-commerce giant formed its own online health service, Alibaba Health Information Technology Ltd., in conjunction with Alipay.[11]

---

[8] https://forkast.news/wp-content/uploads/2019/12/Forkast.Insights-China-Blockchain-Report-2019-2020.pdf

[9] https://forkast.news/wp-content/uploads/2019/12/Forkast.Insights-China-Blockchain-Report-2019-2020.pdf

[10] https://www.ledgerinsights.com/health-blockchain-baidu-medical/

[11] https://forkast.news/baidu-alibaba-tencent-china-health-care-blo/

Alibaba's Blockchain Medical Solution is based on Alibaba Cloud Blockchain Service (BaaS) and Alipay's Ant blockchain technology, which allow hospitals to oversee prescriptions, pharmacist reviews, drug deliveries, drug payments, and medical process supervision. In the future, additional data—including patient information, prescription information, and drug circulation information—will be encrypted and desensitized by blockchain technology (such as zero-knowledge proof, multipart secure computing, and homomorphic encryption). These safeguards will ensure prescriptions are not tampered with to ensure the integrity of patients' multi-channel drug purchases. Blockchain technology also supports the precise matching of electronic prescriptions and patients' conditions, eliminating problems such as prescription modification or abuse. Other advantages of blockchain electronic prescriptions include distributed storage, prescription ledger tracking, easily traceable records written in ledgers (which is convenient for supervision), and an ability to ensure the effectiveness of one-time prescriptions.

Tecent's Blockchain for Healthcare

Tencent is collaborating with Waterdrop, a crowdfunded health insurance firm, to develop a blockchain-powered medical and insurance solution. Tencent plans to integrate this functionality into its WeChat messenger, meaning the platform's 1 billion-plus active monthly Chinese users can access medical bills efficiently and securely. The solution will also benefit medical institutions and insurance firms by facilitating an efficient billing system and a platform for secure, auditable storage of medical information to prevent claims from fraudulent invoices.[12]

In November 2019, Tecent launched its "electronic health card + blockchain" solution in Anhui. Blockchain technology will dramatically change medical data storage and transmission practices in China. It will provide medical institutions with fast and safe information channels and promote data resource integration across departments, institutions, and regions. These developments will help create a nationwide "big network" of health records with the citizenry's personal health at its core. This network will oversee various health-related factors, realize multi-channel, dynamic data collection, and build systematic, structured full life cycle health files.[13]

North America Blockchain for Healthcare

Gartner coined the phrase "trough of disillusionment" to describe an industry's growing pains with new technology implementation. The North American healthcare sector's approach to blockchain appears to be a clear example of this principle. Blockchain technology applications in North American healthcare settings show promise for solving some issues (such as EHR data distribution and nationwide interoperability). However, more research, trials, and experiments must be undertaken to ensure a secure and established system is built before using the technology on a wider scale.[14]

[12] https://forkast.news/baidu-alibaba-tencent-china-health-care-blo/
[13] http://www.ah.chinanews.com/news/2019/1121/234259.shtml
[14] https://www.healthcare.digital/single-post/2020/01/29/Digital-Health-Hype-Cycle-2020

USA - MedRec EHR Blockchain for Healthcare

MedRec is a blockchain EHR system created at the Massachusetts Institute of Technology (MIT). The EHR system focuses on medical data access and permission management and is actively being tested and developed at the Beth Israel Deaconess Medical Center. Eventually, it may be the first EHR system implemented in an HDO.[15/16]

Canada - University Health Network (UHN) Blockchain for Healthcare

In Canada, the largest health research organization in North America—the University Health Network (UHN)—launched a blockchain health record platform in 2018. In collaboration with IBM and eHealth Ontario, the UHN blockchain manages access permissions to patient health data. It also provides a mobile app interface that allows patients unprecedented control over their healthcare records. Patients can choose to enable family members or other HDOs to access specific parts of their health records and withdraw consent at any time.[17]

Discussion

Blockchain technology could transform healthcare as we know it. Its application in medical research, supply chain management, and telehealth offers advantages to researchers, health care providers, and patients. Furthermore, healthcare blockchain integration could expand health data acquisition to populations currently under-served by HDOs.

Additionally, data collection from wearable and mobile devices could provide HDOs with valuable information to improve patient diagnosis and treatment—resulting in better outcomes. For example, HDO abilities to obtain real-time data on blood pressure, blood sugar levels, and heart health would provide HDOs with information that could significantly improve patient care standards.

Big data's use in healthcare aims to improve patient safety and clinical outcomes and promote wellness and disease management. Real-time data collection and big data analytics can enhance big data access and use, which is particularly useful in predictive analytics. Predictive analytics examines and extrapolates old or summarized healthcare data to identify relationship patterns to predict the future. Finally, data mining can identify hidden patterns in health data to anticipate medical risks, predict patient outcomes, and improve health-related services.

Blockchain also provides enhanced privacy and security in telehealth settings. Telehealth provides healthcare to people who cannot easily access these services in person (which is particularly true in the current pandemic). Telehealth platform providers using videoconferencing capabilities and leveraging cloud and internet technologies—coupled with remote patient monitoring mechanisms—provide immense privacy and security challenges that blockchain can help address.

---

[15] https://ieeexplore.ieee.org/document/7573685

[16] https://medrec.media.mit.edu/

[17] https://www.ibm.com/blogs/think/2019/08/bringing-blockchain-to-healthcare-for-a-new-view-on-data/

Conclusion

Blockchain technology is a decentralized network with potential applicability in the healthcare sector (which commonly processes and manages sensitive data). This paper examined blockchain's current utilization in medical research, supply chains, finance, and telehealth. Blockchain can also aid in the interoperability of medical systems and big data acquisition and analysis to provide a foundation for advances in patient care and management.

In today's pandemic-impacted environment, blockchain can provide a cornerstone for a secure telehealth system and benefit patients and HDOs. Blockchain technology use has a place in healthcare's IT ecosystem, and its integration should be researched and adopted.

References

Arsene, C. (2020). *The Global "Blockchain in Healthcare" Report: the 2020 ultimate guide for every executive*. Healthcare Weekly. Retrieved from: https://healthcareweekly.com/blockchain-in-healthcare-guide/

Arunkumar, S. and Muppidi, S. (2019). *Secure your blockchain solutions*. Retrieved from: https://developer.ibm.com/articles/how-to-secure-blockchain-solutions/

Archer, D.W., Bogdanov, D., Kamm, L., Lindell, Y., Nielsen, K., Pagter, J.I., Smart, N.P., and Wright, R.N. (2018). *From Keys to Databases—Real-World Applications of Secure Multi-Party Computation*. The Computer Journal.

Bambara, J.J., and Allen, P.R. (2018). *Blockchain a Practical Guide to Developing Business, Law, and Technology Solutions*. McGraw Hill Education. New York NY.

Chen, H.S., Jarrell, J.T., Carpenter, K.A., Cohen, D.S., and Huang, X. (2019). *Blockchain in Healthcare: A Patient-Centered Model*. Biomed J Sci Tech Res. Vol. 20, No. 3.

Davis, J. (2019). *The 10 Biggest Healthcare Data Breaches of 2019, So Far*. Health IT Security. Retrieved from: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far

2020 DBIR - Data Breach Investigations Report. Retrieved from: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/

Dimitrov, D.V. (2019). *Blockchain Applications for Healthcare Data Management*. Healthcare Informatics Research. Vo. 25, No.1 P 51-56.

Katuwal, G.J., Pandey, S., Hennessey, M., and Lamichhane, B. (2018). *Applications of Blockchain in Healthcare: Current Landscape & Challenges*. arXiv:1812.02776 Vol. 6 No. 1.

Khezr, S., Moniruzzaman, M., Yassine, A., and Benlamri, R. (2019). *Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research*. Applied Sciences. Vol. 9, 1736; doi:10.3390/app9091736

Kuo, T., Kim, H., and Ohno-Machado, L. (2017). *Blockchain distributed ledger technologies for biomedical and health care applications*. Journal of the American Medical Informatics Association, Vol. 24, No. 6.

Linn, L.A. and Koo, M.B., M.D. (2016). *Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research*. True Value Metrics. Retrieved from: http://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/11-74-ablockchainforhealthcare.pdf

Osborne, C. (2020). *The latest healthcare data breaches in 2019/2020*. The Daily Swig: Cybersecurity News and Views. Retrieved from: https://portswigger.net/daily-swig/the-latest-healthcare-data-breaches

Panner, M. (2019). *Blockchain In Healthcare: How It Could Make Digital Healthcare Safer And More Innovative*. Forbes. Retrieved from: https://www.forbes.com/sites/forbestechcouncil/2019/06/18/blockchain-in-healthcare-how-it-could-make-digital-healthcare-safer-and-more-innovative/

Park, J.H. and Park, J.H. (2017). *Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions*. Symmetry. Vol. 9, No. 164. Retrieved from: https://www.mdpi.com/journal/symmetry

Seliem, M. and Elgazzar, K. (2019). BIoMT: *Blockchain for the Internet of Medical Things*. Conference Paper. Retrieved from: https://www.researchgate.net/publication/333633434

Shah, M. and Kondaka, S.S. (2018). *Blockchain for Healthcare: An opportunity to address many complex challenges in healthcare*. CitiusTech.

Siwicki, B. (2019). *How Blockchain Can Protect Telemedicine Programs*. Healthcare IT News. Retrieved from: https://www.healthcareitnews.com/news/how-blockchain-can-protect-telemedicine-programs

Stagnaro, C. (2017). *White Paper: Innovative Blockchain Uses in Health Care*. Freed Associates. Retrieved from: https://www.freedassociates.com/wp-content/uploads/2017/08/Blockchain_White_Paper.pdf

U.S. Department of Commerce. (2016). *2016 Top Markets Report: Pharmaceuticals*. Retrieved from: https://legacy.trade.gov/topmarkets/pdf/Pharmaceuticals_Executive_Summary.pdf

Wabo, B. (2019). *How blockchain can ensure security and compliance in telemedicine*. Enterprise IoT Insight. Retrieved from: https://enterpriseiotinsights.com/20190903/channels/opinion/how-blockchain-can-ensure-security-and-compliance-in-telemedicine

Yaga, D., Mell, P., Roby, N., and Scarfone, K. (2018). *Blockchain Technology Overview*. National Institute of Standards and Technology Internal Report 8202. Retrieved from: https://doi.org/10.6028/NIST.IR.8202

Yao, Y., Rasmus-Vorrath, J., and Angelov, I. (2018). *Blockchain Security and Demonstration*. Retrieved from: https://www.academia.edu/35349686/Blockchain_Security_and_Demonstration