International Journal of Healthcare Information Systems and Informatics
Volume 15 • Issue 3 • July-September 2020

Blockchain in Healthcare
Opportunities, Challenges, and Possible Solutions

Cornelius Chidubem Agbo, University of Ontario Institute of Technology, Canada
Qusay H. Mahmoud, University of Ontario Institute of Technology, Canada

ABSTRACT

Blockchain, an immutable ledger or database shared by peers in a network, is comprised of records of events or transactions that are appended chronologically. Introduced via Bitcoin to the world, blockchain is increasingly being accepted and adopted in different industries and for diverse use cases. Among key industries, health care offers several significant opportunities for applying blockchain conceptualization. Chief areas for health care blockchain applications include electronic medical records management, pharmaceutical supply chain management, biomedical research and education, remote patient monitoring, health insurance claim processing, and health data analytics. Even so, applying blockchain concepts in health care is not without challenges, including interoperability, security-privacy, scalability-speed, and stakeholders' engagement issues. While these challenges may militate against blockchain applications in health care, there are possible countermeasures and implementation techniques, which if adhered to, can reasonably contain many aspects of such challenges.

KEYWORDS

Blockchain, Challenges and Solutions, Distributed Ledger, Electronic Medical Records (EMR), Health Care, Health Data Analytics, Healthcare Opportunities

1. INTRODUCTION

In advocating personalized and proactive care, healthcare services today must leverage the knowledge hidden in massive data that are generated from various medical monitoring devices and patient medical records (PMRs). The transformation of data into knowledge is the hallmark of modern medicine. Such knowledge offers significant potentials to be utilized for promoting personalized treatments (Shae & Tsai, 2018) and for early disease detection in predictive analytics (Agbo, Mahmoud & Eklund, 2018a; 2018b). Yet, efforts to derive knowledge out of data may be futile if these data are siloed in different databases with little or no interoperable capabilities; moreover, such data may be stored in formats that make data sharing difficult. Also, the collected data may be incomplete, unreliable or potentially compromised (Mettler, 2016). Meanwhile, access to the medical data by the healthcare stakeholders must still be controlled, as the security and privacy of patient data must be protected. Hence, modern healthcare services must be designed to be collaborative, open and transparent, without compromising the integrity of the data or the privacy of patients, the ultimate owners and providers of these data.

Current health data management solutions do not sufficiently address many of these critical data requirements. For example, PMRs are usually held by healthcare providers such as hospitals without the patients having full access to the data (Engelhardt, 2017). Accordingly, patients cannot examine their medical data or even share these with new providers to create a complete medical history. This made it difficult for new healthcare providers to construct a patient's medical history. They sometimes

DOI: 10.4018/IJHISI.2020070105

rely on a patient's recollection of their medical history by querying the patient. Yet, this approach is rudimentary and may not result in a complete medical history as the patient may have forgotten details of his past medications and/or may not be able to recount them comprehensively due to lack of knowing proper medical terminologies. Incomplete medical history, as stated earlier, will make it impossible to realize the full potentials of the emerging database technologies for health care. It may also affect the provider's ability to conduct accurate diagnosis and to proffer the right medical intervention. To facilitate the creation and sharing of the complete medical history of patients, care providers should be able to collaborate and exchange patients' information among each other.

With cloud computing (CC), healthcare providers, including hospitals, now make use of patient portals (PP) to connect and exchange data among themselves and with patients. Even so, the cloud-assisted health data exchange environment has drawbacks with respect to data security and privacy. First, hosting patients' data on the cloud exposes them to security vulnerabilities, which could result in data loss or manipulation. Although there exist countermeasures such as cryptographic techniques, which can be employed to protect the data on the cloud, the fact that the cloud storage is centralized still retains some vulnerabilities, for example, the ransomware attack (McCarthy, 2016). Second, to safeguard patient privacy, the patients themselves must be involved and actively participate in the creation, management and sharing of their personal medical data (Kitson, Marshall, Bassett & Zeitz, 2013). Patient-centric medical data management ensures that patients have access to their complete medical history and can decide when, how and with whom to (or not to) share the data.

The blockchain technology, along with the application layer services it supports, promises to offer a distinct solution to address the multiple challenges faced by the current healthcare systems. Blockchain can, in a collaborative and open atmosphere, enable the patient-centered medical data management. Without violating the privacy of the patients, other stakeholders are able to contribute, and to have some level of access, to the medical data. Introduced via Bitcoin to the world (Nakamoto, 2008), blockchain is a distributed ledger technology that has the peculiar advantage of being able to connect distributed stakeholders directly without the need for a trusted third party (TTP). This blockchain characterization will promote low-cost, rapid, and more efficient means of data sharing and collaboration among distributed stakeholders. With its successful application in Bitcoin and other cryptocurrencies, the utility of blockchain can now be exported to non-financial use cases (Burniske, Vaughn, Cahana & Shelton, 2016).

Health care, in fact, represents a significant area where several opportunities exist for the application of blockchain concepts. In biomedical research and education, blockchain has been successfully applied in several use cases. In clinical trials, for instance, blockchain can be applied to prevent the manipulation of clinical research outcomes (Radanović & Likić, 2018). Indeed, as blockchain allows for health data anonymization, patients can be encouraged to make their health data available for clinical studies (Boulos, Wilson & Clauson, 2018) and the integrity of these data can be certified on the basis of the immutability of blockchain. Moreover, given the transparent and open nature of blockchain, research generated from blockchain-based data would be easier to replicate. There is also the potential for blockchain to revolutionize peer-review process for clinical research publications based on its properties of transparency, immutability and decentralization (Roman-Belmonte, De la Corte-Rodriguez, Rodriguez-Merchan, la Corte-Rodriguez, & Carlos Rodriguez-Merchan, 2018). Similarly, Funk, Riddell, Ankel & Cabrera (2018) make a case for the potential use of blockchain in health professions education (HPE).

Given the novelty of blockchain, uncertainties remain in future healthcare applications. Hence, it is paramount for both healthcare researchers and practitioners to understand the opportunities that blockchain presents, the challenges that militate against the development of blockchain-based healthcare applications and how these challenges may be mitigated. In light of this, and based on recent studies in related subject areas, this paper presents the opportunities, challenges and possible solutions, for promoting the use of blockchain in health care. The remainder of this paper is organized as follows. Section 2 provides a brief background of the blockchain technology. In section 3, opportunities for

the application of blockchain in health care are presented. Section 4 discusses the challenges and possible solutions. Finally, section 5 concludes the paper.

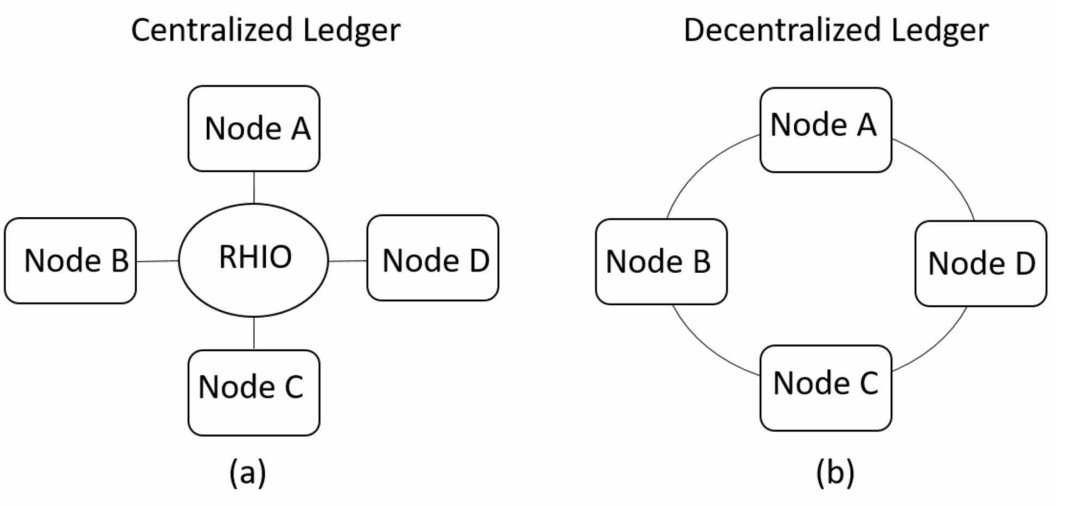
2. BACKGROUND

As noted, the fact that blockchain removes the need for a centralized TTP in distributed applications is why and what made blockchain unique. By using distributed consensus protocols such as the proof of work (PoW) protocol (Nakamoto, 2008), blockchain makes it very easy for participating stakeholders to verify its cumulative contents while ensuring great difficulties for anyone trying to alter any part of the previously added contents. Along with decentralization, blockchain also features other interesting properties that are useful in developing healthcare services and applications. This section overviews the peculiar blockchain properties and explains how they can benefit healthcare applications.

Decentralization, as a property of blockchain, ensures that every party in a distributed network has an identical copy (or ledger) of complete records of events or transactions, without any single entity having a singular authority over the true state of the records. Traditionally, distributed applications have relied on a TTP, for example, a bank in financial transactions or the Regional Health Information Organization (RHIO) (Adler-Milstein, Bates & Jha, 2009) in the case of health care, to exchange information and to maintain the true state of the distributed ledgers. The distinction between the centralized system that relies on TTP and the blockchain-based decentralized system that relies on distributed consensus protocol is illustrated in Figure 1. Decentralization removes the need for a TTP, thereby eliminating the single point of failure. This improves transactions speed, and reduces transaction costs by the removal of the TTP-charged transaction fees.

Immutability, which ensures that data saved on blockchain cannot be modified without being detected, is another interesting property of blockchain. Adding records to the blockchain involves the use of a cryptographic hash function. A hash function takes a message of arbitrary length to produce a unique output of a fixed length, thus, no two different messages can produce the same output. To add records to the blockchain, the set of records or transactions that are created within a period are put together into a block and appended to the blockchain. After the first block has been created, every subsequent block must contain, in addition to the transactions, the hash output of the previous block,

Figure 1. Centralized vs decentralized ledger. In (a), there are multiple ledgers but all records are held in the TTP (bank), whereas in (b), there is only one ledger, but every node has some level of access to that ledger.



as shown in Figure 2. By embedding the hash value of a block in the subsequent block, it ascertains that any modification to the content of the block can be detected using the hash value saved on the subsequent block.

Further, each participant in a blockchain network has a pair of public and private keys (Housley, 2004). With these keys, it is possible to encrypt the data on the blockchain in such a way that only the users with the right access permissions can decrypt the data. Hence, even though users in a blockchain network can verify algorithmically that they have the true copies of the distributed ledger, for privacy reasons, they may not have access to all the records in the ledger. Importantly, blockchain has the property of transparency and openness but at the same time provides data privacy and security. Additionally, when records are created in a blockchain, they are time-stamped, and appended sequentially to the blockchain, thereby creating an audit trail of who did what and when.

Altogether, how do these blockchain properties align with the requirements for healthcare applications? The benefits of decentralization to health care are obvious – health care, by its very nature, involves distributed stakeholders that operate independently, including the patients, providers, insurers, other payers (e.g., assigned government agencies) and more. Blockchain-based decentralization would simply ensure all of these stakeholders are directly interconnected with everyone having access to the same health records of patients, without any third-party intermediary. This would facilitate medical data sharing among healthcare stakeholders at reduced costs. There would also be cost savings from, for example, duplicate testing that would be carried out when patients' test results are stored separately in different provider databases without any interoperability. Decentralization allows every stakeholder to have a copy of the complete medical records of the patients. It offers verification via data redundancy created while helping to protect the medical data from accidental losses, corruption and malicious attacks on the data such as the ransomware attack (McCarthy, 2016).

The immutability property of blockchain guarantees the integrity of the medical records since data, once saved on the blockchain, cannot be modified or deleted. The need to protect the integrity of medical records cannot be over-emphasized. Combined with decentralization, transparency and auditability, immutability creates trust among collaborating stakeholders. Trust in the integrity of data is essential for many healthcare use cases such as diagnostics and other clinical research conducted on available and accessible databases. The strong cryptographic protocols employed in blockchain also increase the confidence of the stakeholders in the security and privacy of the health data stored on the blockchain. The cryptographic protocols are used to anonymize the data stored on the blockchain, which further helps to safeguard the needs for data security and privacy.

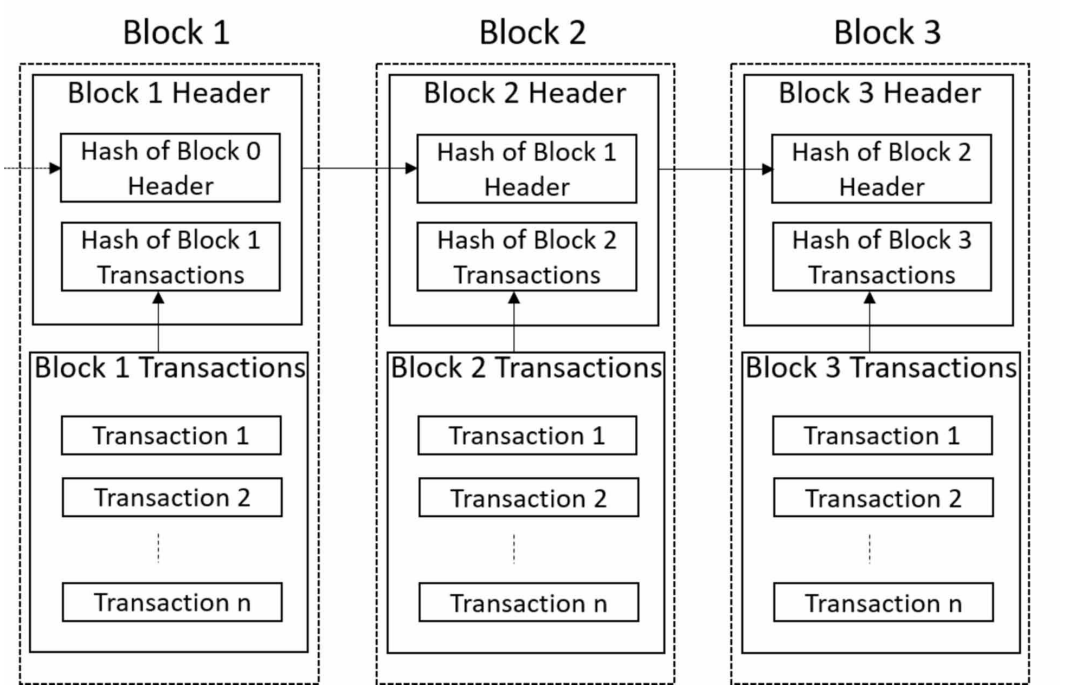
Finally, blockchain supports the definition of rules, known as smart contracts (Swan, 2015), that can be used to set the rules about how the health data can be used by the different stakeholders. Smart contracts are not integral attributes of the blockchain, but they come handy in developing complex blockchain applications, such as for health care. Smart contracts are based on the properties of the blockchain, so they are immutable, once set and can be trusted by the stakeholders to perform reliably throughout its lifetime.

Based on these peculiar properties and features of blockchain and their potential benefits to health care, it is time to examine some specific opportunities for the applications of blockchain in the different domains of the healthcare industry. This is followed by a discussion of the challenges and the possible solutions as summarized in Figure 3.

3. BLOCKCHAIN OPPORTUNITIES IN HEALTHCARE

Based on the special properties of blockchain, it can be seen that blockchain is applicable in use cases that have any of the following characteristics: (a) two or more collaborating stakeholders exist; (b) there are intermediaries that could be removed to improve the security and/or the efficiency of the system: (c) trust among the collaborating entities is needed; (d) data integrity must be maintained,

Figure 2. A simplified example of how blocks are chained to form a blockchain. Notice that each block contains a header and several transactions. The transactions in a block are hashed to generate a fixed-length hash output which is added to the block header. After the creation of the first block, every subsequent valid block must contain the hash output of the previous block header.



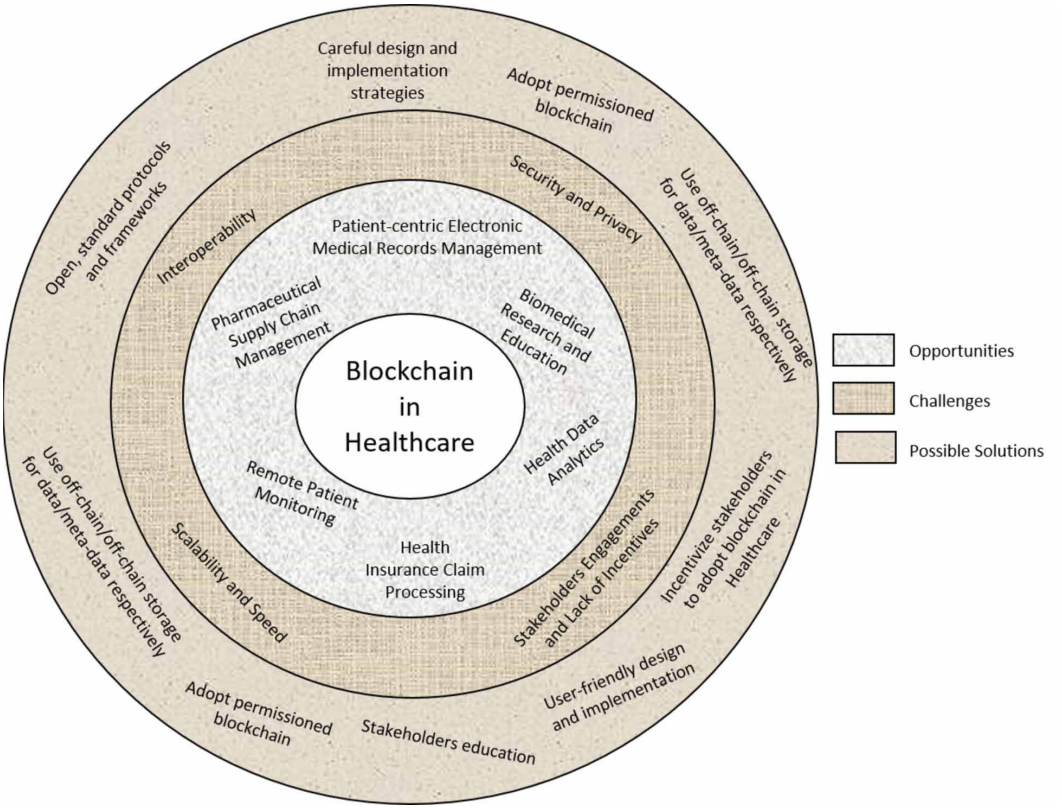
and (e) there is a need for openness and transparency and/or there is a need to promote trust among the collaborating entities.

In the following sub-sections, several healthcare use cases representing opportunities for blockchain applications are discussed. In each case, the healthcare problem is captured and how the blockchain concepts can address the problem is illustrated. While it is not possible to cover an exhaustive list of all the potential areas of blockchain applications in health care, the review should cover those most often considered to be critically relevant.

3.1 Patient-Centric EMR Management

Electronic medical records (EMRs) management is concerned with the electronic creation, storage and management of patients' personal, medical and other health-related data. Capturing clinical interactions between patients and their care providers (as well as health data collected through medical sensors), provide a rich source of information, which can be harnessed to improve healthcare decisions. Yet, as Figure 4 (a) depicts, the current practice in which EMRs are stored across the different providers' databases with little or no interoperability makes it very difficult to take full advantage of these data in improving care delivery. Moreover, there is growing consensus that health data and information related to a patients' health should be readily available to the patients so that they can be active participants in their own care (Kitson et al., 2013). Other healthcare stakeholders also require different levels of access to the medical data and information; nonetheless, there is an increasing agreement that patients should be in control of what information they want to share with other stakeholders and under what conditions. Put simply, the desired solution should be one that is patient-centric, providing the right data to the right stakeholders (patients and authorized care providers) at the right time while guaranteeing the needed security and privacy of the healthcare data being accessed.

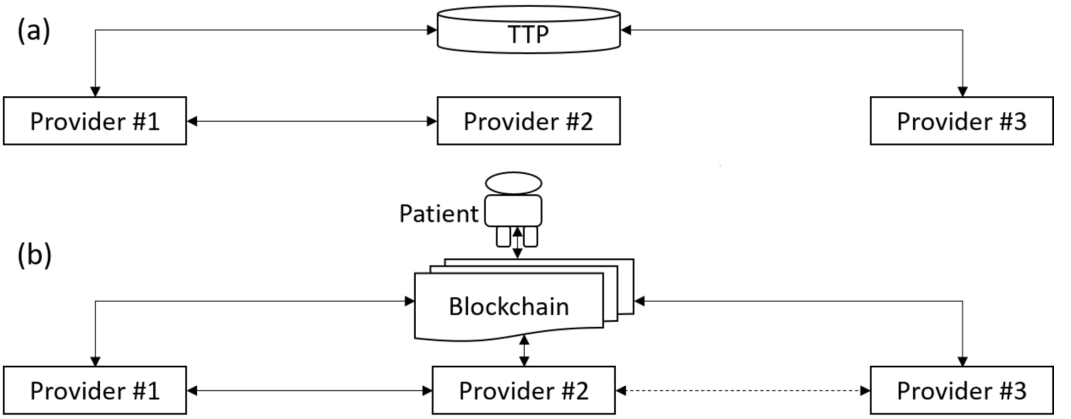
Figure 3. Summary of the opportunities, challenges, and possible solutions



Blockchain potentially offers the best opportunity to realize such a solution – a solution that can put patients at the centre of managing their own health data, improve privacy and regulate access to the medical records while guaranteeing availability, and ultimately ensure data completeness by facilitating the linking and sharing of EMRs among different healthcare stakeholders, as shown in Figure 4 (b). Blockchain, with its unique properties of decentralization, immutability, auditability, reliability, and redundancy, offers many of the key features that make this technology very suitable for realizing the above objectives (Radanović & Likić, 2018).

At this point, key examples of how blockchain is being employed by the emerging blockchain startups to address the management of EMRs will be highlighted. One such example is Guardtime, a blockchain-based platform to secure over 1 million patients records in Estonia (Angraal, Krumholz & Schulz, 2017). Another example is MedRec (Azaria, Ekblaw, Vieira & Lippman, 2016), which aims at giving patients the ability to control who can access their medical record through some fine-grained access permissions built onto the blockchain. The Gem Health Network (GHN) (Mettler, 2016) is yet another example, which is developed by the US company, Gem, using the Ethereum blockchain platform. GHN allows different healthcare practitioners to have shared access to the same data. Healthbank, a Swiss digital health company, is similarly working on empowering patients to be in full control of their data using the blockchain platform (Mettler, 2016). There is also the MedicalChain project (Engelhardt, 2017), whose blockchain-based platform will facilitate the sharing of patients medical records across international healthcare institutions, and the Healthcoin initiative (Engelhardt, 2017), which aims at constructing a global EMR system. Other recently developed blockchain-based EMR applications include the Ancile (Dagher, Mohler, Milojkovic, Marella & Marella, 2018), MedBlock (Fan, Wang, Ren, Li & Yang, 2018), BlockHIE (Jiang, Cao, Wu, Yang, Ma & He, 2018), and FHIRChain (Zhang et al., 2018).

Figure 4. Comparison of existing EMR system with blockchain-based patient-centric EMR system. 4 (a) shows a case where a patient is seeing three different providers. Provider #1 and #3 can share data through a trusted third-party (TTP), e.g., Regional Health Information Organization (RHIO) with the limitations of TTP as discussed in section 2. Alternatively, two providers can exchange data if they are on the same network, i.e., have some business relationships, as in #1 and #2. Providers #2 and #3 may not be able to exchange data because they are not connected through a TTP and they are not on the same network. 4 (b) shows how this problem is resolved with blockchain which allows the patient to retrieve his data from all the three providers whenever he wants and to authorize the sharing of the data with anyone he chooses through the blockchain-enabled smart contracts. Therefore, data can be exchanged between #2 and #3 even though they do not have a business relationship, and without going through a TTP.



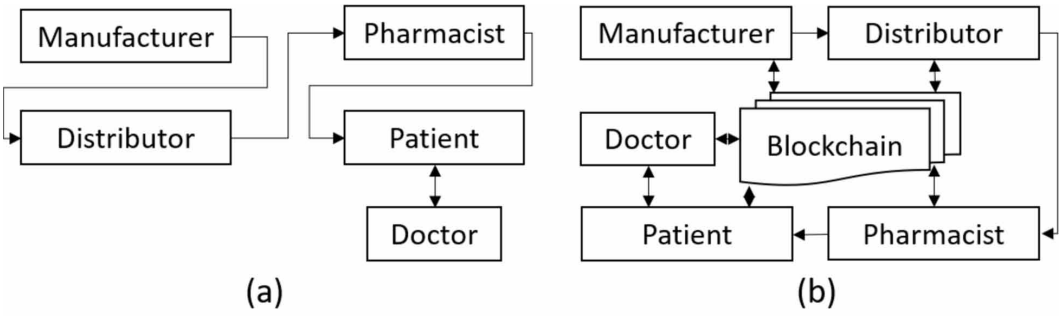
3.2 Pharmaceutical Supply Chain Management (SCM)

Pharmaceutical supply chain management (SCM), particularly in drug production and distribution, is a domain ripe for applying blockchain conceptualization. The delivery of counterfeit or substandard medications can have dire consequences for patients. Yet, this is a common problem faced in the pharmaceutical industry. According to the World Health Organization (WHO) data, up to ten percent (10%) of drugs in circulation worldwide are counterfeit, and this number is said to be even much higher (up to 30%) in developing countries (Barbereau, 2010).

The unique properties of transparency, openness, immutability, data provenance, time-stamping and auditability inherent in blockchain come handy in ensuring that the counterfeiting problem in the drug manufacturing and distribution industry can be contained. Once a drug is produced, it is marked and recorded on the blockchain with a timestamp, which in turn creates an irrefutable and immutable proof of who produced the drug, when and where the drug was produced. The distribution and the transfer of ownership of the drugs from the point of production through the distribution chains to the final consumers (the patients) can then be tracked on the blockchain in a way that is transparent to all stakeholders. With this approach, it is impossible to produce and distribute counterfeit drugs. Poor quality drugs can always be traced back to the producer and even stolen drugs can be tracked provided the drugs are registered on the blockchain upon production. Figure 5 illustrates how the blockchain technology can overcome the drug-counterfeiting challenge.

The Counterfeit Medicines Project (Mettler, 2016) focuses on using blockchain to fight counterfeit medications. Modum.io AG is a company that has developed a blockchain-based application for pharmaceutical SCM. The application uses blockchain to achieve data immutability while creating public accessibility of the temperature records of pharmaceutical products during their transportation so that their compliance to quality control temperature requirements may be verified (Bocek, Rodrigues, Strasser & Stiller, 2017). Discussion of emerging prototypes and research initiatives related to the application of blockchain in the area of pharmaceutical SCM may be found in Mackey & Nayyar (2017).

Figure 5. An illustration of how blockchain can solve the drug counterfeiting problem. In (a), as the drug flows from the manufacturer to the patient through the distributor and the pharmacist, there is the possibility of counterfeiting the original drug at any stage of the process by changing the labels, the expiry date, etc. Without a feedback system, there is no way any modification can be detected. Similarly, there is no mechanism for the pharmacist to know that the prescription given to the patient by the doctor has not been altered. In (b), the blockchain is used to overcome these potential loopholes. Every drug is registered to the blockchain and all the stakeholders are connected to the blockchain and can confirm the validity of any product or information they receive.



3.3 Remote Patient Monitoring

Remote patient monitoring (RPM) involves the collection of biomedical data through body area sensors via the Internet-of-Things (IoT) and mobile devices. RPM can remotely monitor the status of a patient outside traditional healthcare environments such as hospitals. As RPM has to do with remote collection and transmission of sensitive health data, a major challenge for RPM applications is how to collect and transmit the data securely while preserving the privacy of patients concerned. Here, blockchain has been proposed as a means to achieve the secure transmission, storage, sharing and retrieving of the remotely-collected biomedical data (Dey, Jaiswal, Sunderkrishnan & Katre, 2017).

To date, some authors have demonstrated how smart contracts on the Ethereum blockchain platform can support real-time patient monitoring application with the capability to provide automated interventions in a secure environment (Griggs et al., 2018). Similarly, blockchain is employed to develop SMEAD, a mobile-enabled assisting device for monitoring diabetes patients (Saravanan, Shubha, Marks & Iyer, 2017). Uddin, Stranieri, Gondal & Balasubramanian (2018) developed a blockchain-based patient-centric agent (PCA) to achieve end-to-end data security and privacy in a continuous RPM application. Additionally, Ji, Zhang, Ma, Yang & Yao (2018) have proposed a scheme known as BMPLS (Blockchain-based Multi-level Privacy-preserving Location Sharing) for realizing privacy-preserving location sharing for RPM application.

3.4 Health Insurance Claim Processing

Insurance claims processing in health care can benefit from blockchain's unique features of transparency, decentralization, immutability and auditability of records storage (Boulos et al., 2018). Many authors identify insurance claim processing as a very promising area for the application of blockchain technology (Angraal, Krumholz & Schulz, 2017; Gordon & Catalini, 2018; Boulos et al., 2018; Roman-Belmonte, Corte-Rodriguez, Rodriguez-Merchan, Corte-Rodriguez & Rodriguez-Merchan, 2018). However, specific instances of prototype implementations of such systems are still very limited. One good example is the MIStore (a blockchain-based medical insurance storage system) which is deployed on the Ethereum blockchain platform (Zhou, Wang & Sun, 2018). Also, Engelhardt (2017) highlights an initiative by a company named Pokitdok that aims to partner with Intel to build a blockchain-based system that will facilitate insurance claim resolution in health care.

3.5 Health Data Analytics

Blockchain provides a unique opportunity to harness the power of other emerging technologies such as deep learning and transfer learning techniques to realize predictive analytics of healthcare data and advance the research in the area of precision medicine (Shae & Tsai, 2018).

Boulos et al. (2018) and Roman-Belmonte et al. (2018) also noted such a use case for blockchain application in health care whereas Mamoshina et al. (2017) provides a comprehensive roadmap on how the use of blockchain in health data analytics can be realized in an intelligent fashion. Juneja and Marefat conducted experimental research in which blockchain is used in a deep-learning architecture for arrhythmia classification (Marefat & Juneja, 2018).

4. CHALLENGES AND POSSIBLE SOLUTIONS

Despite the attractiveness of blockchain-associated properties and potential benefits in blockchain-based healthcare applications, it is important to note that the technology is not without limitations. Challenges exist that militate against the successful use of blockchain technology in health care. Some of these challenges are discussed here, with suggested potential solutions to overcome them.

4.1 Interoperability

The interoperability challenge stems from the fact that there is not yet a universal standard for developing blockchain-based healthcare applications; for example, applications developed by different vendors or on different platforms may not be interoperable. Consequently, there is a need to develop protocols that would ensure interoperability between blockchain networks and that would facilitate consistent storage of medical records and the seamless transfer of such records across different platforms. Current efforts are focused on developing prototypes and proofs-of-concept with less attention paid to the need for interoperability. The resulting systems are disparate blockchain-based healthcare platforms with varying levels of smart contract functionality, transaction schemes, and consensus models.

Compare and contrast, for example, HealthChain (Ahram, Sargolzaei, Sargolzaei, Daniels & Amaba, 2017) which is an EMR application developed as a permissioned, private blockchain network via the IBM Blockchain's Hyperledger Fabric (Androulaki Artem Barger Vita Bortnikov et al., 2018) v. the Ancile blockchain framework (Dagher et al., 2018), which similarly utilizes smart contracts to control EMR management, but is built on the Ethereum (Ethereum, 2015) blockchain platform. These two systems manage EMRs on very different platforms; as such, without a well-defined standard, it is difficult to transfer a patient's record from one platform to the other. As data sharing is at the heart of the design of modern EMR management systems, the whole advantage of blockchain is lost if disparate blockchain networks cannot interoperate among each other in order to exchange critically stored data.

One possible solution to the interoperability problem is to develop standard protocols that can guarantee interoperability between different blockchain products. For blockchain technology to be fully adopted and deployed in operational healthcare environments, open standards for interoperability need to be defined. Importantly, researchers should start collaborating on overcoming the interoperability issues and the standardization processes. A standards group (ISO/TC 307) currently exist to which researchers can send in their contributions (ISO, 2018). Some early research into the interoperability of blockchain has produced two broad categories of interoperability solutions, namely open protocols and multi-chain frameworks (Curran, 2018). On the one hand, the open protocols are standards that define how blockchains can interoperate and exchange data among themselves, for example, Interledger (https://interledger.org/). Multi-chain frameworks, on the other hand, are open environments that different blockchain networks can plug into and be able to exchange information, for example, Polkadot (https://polkadot.network/) and Cosmos (https://cosmos.network/).

4.2 Security and Privacy

When it comes to security, it is evident that no one system is perfectly secure. So, even though state-of-the-art encryption techniques are employed in the blockchain, there are still potential security breaches that may be exploited to compromise the data stored on the blockchain. One famous security threat in blockchain is the 51% attack, which happens when the malicious nodes in a blockchain network outnumber the honest nodes (Kalis, Leong, Mitchell, Pupo & Truscott, 2016). Under such a circumstance, the malicious nodes may be able to modify the data on the blockchain by undermining the distributed consensus mechanism, thereby nullifying the immutability property of blockchain.

Another security challenge is the fact that information access in the blockchain is via the private keys, which are prone to potential security breaches. On the one hand, if these private keys are stolen, it could result in unauthorized access to the stored health data; on the other hand, if the keys are lost, the stored data cannot be accessed. There is also the concern on the emergence of future technologies such as quantum computing that will be able to break the current encryption technologies upon which the blockchain is based (Engelhardt, 2017).

On privacy, the blockchain promotes transparency at the expense of confidentiality. Here, there is a concern that despite the anonymity introduced by using hashed values as public addresses, it is still possible to unveil the identity of a patient in a public blockchain by linking together sufficient data that are associated to that patient (Radanović & Likić, 2018). Moreover, there is also the potential risk of security breaches that could arise from intentional malicious attacks to the healthcare blockchain by criminal organizations or even government agencies that could compromise the privacy of the patients. Indeed, several cases of reported attacks on the blockchain-based cryptocurrencies have been reported to date (Yli-Huumo, Ko, Choi, Park & Smolander, 2016). Given the sensitive nature of healthcare data, any viable solution for managing EMRs must ensure both the integrity of the stored data and the protection of the patient's privacy.

Potential solutions to the aforementioned security and privacy-related challenges consist in following a careful design and implementation techniques for blockchain-based healthcare applications to mitigate the identified challenges. For example, through the adoption of a permissioned blockchain network such as the private or consortium blockchain like ModelChain (Kuo & Ohno-Machado, 2018) instead of the public blockchain like Bitcoin, the problem of 51% attack is reasonably overcome and contained because arbitrary malicious nodes cannot hijack the network as only the authorized (honest) nodes can participate in the ModelChain network.

Similarly, another technique to mitigate the privacy issue is to store only the encrypted pointers to the real data on the blockchain, while storing actual data off-blockchain, and using the smart contracts (Swan, 2015) to automate the data management protocols as exemplified in HealthChain (Ahram et al., 2017) and Ancile (Dagher et al., 2018). Moreover, following a rigorous software development process and applying all known security measures during code development go a long way in containing most of the security threats.

In the end, blockchain cannot fully stop all the potential attacks in healthcare cybersecurity, basically because the healthcare data would still have to be accessible and readable by the healthcare stakeholders. Accordingly, known security challenges of authentication, authorization, sniffing of credentials and data theft will continue to persist. Nonetheless, blockchain will prove to be very effective in addressing most, if not all, integrity-based attacks because of its immutability characteristics.

4.3 Scalability and Speed

Scalability of blockchain-based healthcare solutions is a well-known challenge especially occasioned by the volume of data involved. It is not optimal, or even possible in some cases, to store the high-volume biomedical data on blockchain as this is bound to cause serious performance degradation. The scalability problem is directly related to the processing speed. Depending on the protocol in use, the blockchain-based processing can introduce some significant latency, which in turn limits

the scalability of the system. For example, the validation mechanism in the current set-up of the Ethereum blockchain platform necessitates all the nodes in a network to participate in the validation process (Yli-Huumo, Ko, Choi, Park & Smolander, 2016). This incurs considerable processing delay, especially if the data load is significant.

Similarly, the Bitcoin-based PoW protocol executes on average 288,000 transactions per day, which is very small when compared to Visa credit card that can execute up to 150 million transactions per day (Kuo, Kim & Ohno-Machado, 2017). Hence, for real-time and scalable healthcare applications, such as continuous RPM, blockchain may proof inefficient. Possible solutions to the scalability and speed problem include the use of blockchain merely as an index for healthcare data, containing only some condensed information about the data and how they can be accessed, while the actual healthcare data is stored off-blockchain (Esposito, De Santis, Tortora, Chang & Choo, 2018; Kaur et al., 2018). However, this countermeasure removes the benefits of redundancy and continuous availability that the blockchain should ordinarily provide for the healthcare data. Further, the speed problem associated with consensus algorithms such as PoW used in some public blockchains can be mitigated by using the permissioned blockchain in which only some nodes are permitted to participate in the consensus and validation processes (Ahram et al., 2017).

4.4 Stakeholders Engagements and Lack of Incentives

Engelhardt (2017) noted that "Blockchain technology is only as good as its users". The technical complexity of blockchain is one of its limitations as some stakeholders may find it difficult to grasp how to use the technology. Despite its many promises, if the blockchain technology is misused, the outcome will be undesirable. For instance, if some invalid or inaccurate data are stored on the blockchain, the immutability property of blockchain will only ensure that the inaccurate data are immutable, which is of no real value in this case. The vision of blockchain in healthcare is to transfer control and ownership of healthcare data to the patients; however, the patients especially the elderly and the young may be unable or unwilling to participate in the management of their health data (Radanović & Likić, 2018). This problem is echoed in Engelhardt (2017) where it is noted that if patients are unaware of what to do with their health data and how to manage them using the blockchain, they will invariably involve others to manage the data for them, which eventually nullifies the whole idea of using blockchain to empower the patients in the control of their personal health data.

A possible solution to stakeholder engagement is to engage in stakeholder education, simplifying the concept of blockchain and how it can be used to better manage healthcare resources. Also, the design and implementation of blockchain-based healthcare applications should then take into serious consideration the utility as well as usability of the system, and the integrity of the data before and after it is stored on the blockchain. Clear incentives should exist to encourage healthcare stakeholders to adopt blockchain-based solutions. There should also be ways to mask the complexity of the underlying blockchain technologies, for example, the private keys should be easy-to-use by the stakeholders but not become easily compromised.

5. CONCLUSION AND FUTURE WORK

In summary, the basic conceptualization of the blockchain technology in terms of its various unique properties and how these blockchain technological features can create opportunities for improvement in different domain of healthcare applications, notwithstanding the inherent challenges to be addressed, have been highlighted here.

Notably, blockchain has the potential to facilitate efficient sharing of healthcare data among stakeholders while guaranteeing the integrity of the medical data and the privacy of the patients. Blockchain has interesting properties that enable it to achieve these objectives, making it useful in the management of EMRs, pharmaceutical SCM, biomedical research and education, RPM applications, health insurance-claim processing, health data analytics and more. However, considerable challenges

and risk factors exist that must be taken into consideration in the application of blockchain technology in health care. These challenges include interoperability, security and privacy, scalability and speed, and stakeholders' engagement. While these challenges may militate against the application of blockchain in health care, there are possible solutions and implementation techniques that, if properly adhered to, can mitigate most of the challenges. As blockchain is a relatively new technology, it suffices to note that the long-term issues associated with the technology have not yet been evaluated.

Areas for future work will consist of developing more proofs-of-concept of blockchain-based healthcare applications to develop a deeper understanding of the strengths and weakness of the systems. Also, further research should be conducted to develop robust solutions to the identified challenges. Finally, the integration of blockchain technology with deep-learning and other emerging artificial intelligence (AI) solutions will ensure that our healthcare systems will be able to interoperate more successfully in a highly secure and private environment to yield meaningful information and knowledge for personalized medicine.

REFERENCES

Adler-Milstein, J., Bates, D. W., & Jha, A. K. (2009). U.S. regional health information organizations: Progress and challenges. *Health Affairs*, *28*(2), 483–492. doi:10.1377/hlthaff.28.2.483 PMID:19276008

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2018a). An Architecture for Cloud-Assisted Clinical Support System for Patient Monitoring and Disease Detection In Mobile Environments. In *Proceedings of the 12th EAI International Conference on Pervasive Computing Technologies for Healthcare - PervasiveHealth '18* (pp. 245–250). New York: ACM Press. doi:10.1145/3240925.3240944

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2018b). A Scalable Patient Monitoring System Using Apache Storm. In *Proceedings of the 2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)* (pp. 1–6). IEEE. doi:10.1109/CCECE.2018.8447696

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J. & Amaba, B. (2017). Blockchain technology innovations. In *Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON)* (pp. 137–141). doi:10.1109/TEMSCON.2017.7998367

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Muralidharan, S. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *EuroSys*, *18*. doi:10.1145/3190508.3190538

Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain Technology Applications in Health Care. *Circulation: Cardiovascular Quality and Outcomes*, *10*(9), e003800. doi:10.1161/CIRCOUTCOMES.117.003800 PMID:28912202

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016* (pp. 25-30). doi:10.1109/OBD.2016.11

Barbereau, S. (2010). Growing threat from counterfeit medicines. *Bulletin of the World Health Organization*. doi:10.2471/BLT.10.020410 PMID:20431784

Benchoufi, M., Porcher, R., Ravaud, P., Benchoufi, M., Porcher, R. & Ravaud, P. (2018). Blockchain protocols in clinical trials: Transparency and traceability of consent. doi:10.12688/f1000research.10531.3

Bocek, T., Rodrigues, B. B., Strasser, T., & Stiller, B. (2017, May). Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In *Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)* (pp. 772-777). IEEE.

Boulos, M. N. K., Wilson, J. T., & Clauson, K. A. (2018). Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. *International Journal of Health Geographics*, *17*(1), 25. doi:10.1186/s12942-018-0144-x PMID:29973196

Burniske, C., Vaughn, E., Cahana, A., & Shelton, J. (2016). Blockchain Technology Can Enhance Electronic Health Record Operability. ARK Invest. Retrieved from https://ark-invest.com/research/blockchain-technology-ehr

Curran, B. (2018). Looking Ahead to Blockchain Interoperability: Issues & Future Solutions. *Blockonomi*. Retrieved from https://blockonomi.com/blockchain-interoperability/

Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B. & Marella, B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society, 39*(December 2017), 283–297. 10.1016/j.scs.2018.02.014

Dey, T., Jaiswal, S., Sunderkrishnan, S., & Katre, N. (2017). A Medical Use Case of Internet of Things and Blockchain. In *Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 486–491). Academic Press. doi:10.1109/ISS1.2017.8389459

Engelhardt, M. A. (2017). Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. *Technology Innovation Management Review*, *7*(10), 22–34. doi:10.22215/timreview/1111

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. R. (2018). Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? *IEEE Cloud Computing*, *5*(1), 31–37. doi:10.1109/MCC.2018.011791712

Ethereum. Ethereum Project. (2015). Retrieved from https://www.ethereum.org/

Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *Journal of Medical Systems*, *42*(8), 136. doi:10.1007/s10916-018-0993-7 PMID:29931655

Funk, E., Riddell, J., Ankel, F., & Cabrera, D. (2018). Blockchain Technology: A Data Framework to Improve Validity, Trust, and Accountability of Information Exchange in Health Professions Education. *Academic Medicine*, *1*. doi:10.1097/ACM.0000000000002326 PMID:29901658

Gordon, W. J., & Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. *Computational and Structural Biotechnology Journal*, *16*, 224–230. doi:10.1016/j.csbj.2018.06.003 PMID:30069284

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of Medical Systems*, *42*(7), 130. doi:10.1007/s10916-018-0982-x PMID:29876661

Housley, R. (2004). Public Key Infrastructure (PKI). In *The Internet Encyclopedia*. Hoboken, NJ, USA: John Wiley & Sons, Inc. doi:10.1002/047148296X.tie149

ISO. (2018). ISO/TC 307 - Blockchain and distributed ledger technologies. Retrieved October 3, 2018, from https://www.iso.org/committee/6266604.html

Ji, Y., Zhang, J., Ma, J., Yang, C., & Yao, X. (2018). BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems. *Journal of Medical Systems*, *42*(8), 147. doi:10.1007/s10916-018-0998-2 PMID:29961160

Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M. & He, J. (2018). BlockHIE: a BLOCkchain-based platform for Healthcare Information Exchange. doi:10.1109/SMARTCOMP.2018.00073

Kalis, C. B., Leong, C., Mitchell, E., Pupo, E., & Truscott, A. (2016). Blockchain : Securing a New Health Interoperability Experience. In *Proceedings of the NIST Workshop on Blockchain & Healthcare*. doi:10.1001/jama.2012.362.4

Kaur, H., Alam, M. A., Jameel, R., Kumar Mourya, A., Chang, V., Alam, M. A., & Chang, V. et al. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *Journal of Medical Systems*, *42*(8), 156. doi:10.1007/s10916-018-1007-5 PMID:29987560

Kitson, A., Marshall, A., Bassett, K., & Zeitz, K. (2013). What are the core elements of patient-centred care? A narrative review and synthesis of the literature from health policy, medicine and nursing. *Journal of Advanced Nursing*, *69*(1), 4–15. doi:10.1111/j.1365-2648.2012.06064.x PMID:22709336

Kuo, T.T. & Ohno-Machado, L. (2018). ModelChain: decentralized privacy-preserving healthcare predictive modeling framework on private Blockchain networks. Doi:10.3969/j.issn.1002-5006.2016.00.000

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211–1220. doi:10.1093/jamia/ocx068 PMID:29016974

Mackey, T. K., & Nayyar, G. (2017). A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert Opinion on Drug Safety*, *16*(5), 587–602. doi:10.1080/14740338.2017.1313227 PMID:28349715

Mamoshina, P., Ojomoko, L., Yanovich, Y., Ostrovski, A., Botezatu, A., Prikhodko, P., & Zhavoronkov, A. et al. (2017). Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. *Oncotarget*, *9*(5), 5665–5690. doi:10.18632/oncotarget.22345 PMID:29464026

Marefat, M., & Juneja, A. (2018). Leveraging Blockchain for Retraining Deep learnign Architecture in Patient-Specific Arrhythmia Classification. In *Proceedings of the 2018 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI)* (pp. 393–397). IEEE.

McCarthy, J. (2016). MedStar attack found to be ransomware, hackers demand Bitcoin. Healthcare IT News. Retrieved from https://www.healthcareitnews.com/news/medstar-attack-found-be-ransomware-hackers-demand-bitcoin

Mettler, M. (2016). Blockchain Technology in Healthcare The Revolution Starts Here. In *Proceedings of the 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom)* (pp. 520–522). IEEE. doi:10.1109/HealthCom.2016.7749510

Mytis-Gkometh, P., Drosatos, G., Efraimidis, P. S., & Kaldoudi, E. (2018). Notarization of knowledge retrieval from biomedical repositories using blockchain technology. In *Precision Medicine Powered by pHealth and Connected Health* (pp. 69–73). Springer Singapore; doi:10.1007/978-981-10-7419-6_12

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. doi:10.1007/s10838-008-9062-0

Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000 Research*, *5*, 2541. doi:10.12688/f1000research.9756.1 PMID:28357041

Radanović, I., & Likić, R. (2018). Opportunities for Use of Blockchain Technology in Medicine. *Applied Health Economics and Health Policy*, *16*(5), 583–590. doi:10.1007/s40258-018-0412-8 PMID:30022440

Roman-Belmonte, J. M., De la Corte-Rodriguez, H., Rodriguez-Merchan, E. C. C., la Corte-Rodriguez, H., & Carlos Rodriguez-Merchan, E. (2018). How blockchain technology can change medicine. *Postgraduate Medicine*, *130*(4), 420–427. doi:10.1080/00325481.2018.1472996 PMID:29727247

Saravanan, M., Shubha, R., Marks, A. M., & Iyer, V. (2017). SMEAD: A secured mobile enabled assisting device for diabetics monitoring. In *Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE. doi:10.1109/ANTS.2017.8384099

Shae, Z., & Tsai, J. (2018). Transform Blockchain into Distributed Parallel Computing Architecture for Precision Medicine. In *Proceedings of the IEEE 38th International Conference on Distributed Computing Systems* (pp. 1290–1299). IEEE. doi:10.1109/ICDCS.2018.00129

Swan, M. (2015). *Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc*. Sebastopol, CA: O'Reilly Media, Inc. doi:10.1016/S0197-4572(81)80089-4

Uddin, M.A., Stranieri, A., Gondal, I. & Balasubramanian, V. (2018). Continuous Patient Monitoring with a Patient Centric Agent: A Block Architecture, *6*. doi:10.1109/ACCESS.2018.2846779

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on Blockchain technology? - A systematic review. *PLoS One*, *11*(10), 1–27. doi:10.1371/journal.pone.0163477 PMID:27695049

Zhang, P., White, J., Schmidt, D. C., Lenz, G., Rosenbloom, S. T., & Zhanga, P. … Rosenbloomc, S.T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Computational and Structural Biotechnology Journal, 16*, 1-30.

Zhou, L., Wang, L., & Sun, Y. (2018). MIStore: A Blockchain-Based Medical Insurance Storage System. *Journal of Medical Systems*, *42*(8), 149. doi:10.1007/s10916-018-0996-4 PMID:29968202

Cornelius Chidubem Agbo received his first degree in Electronic Engineering from the University of Nigeria in 2009. In 2014, he received his MSc degree in Computer Security from Telecom ParisTech, France. He was employed the same year at the University of Nigeria as a Lecturer in Electronic Engineering Department. He is currently pursuing his PhD at the University of Ontario Institute of Technology, Canada, where he is researching on blockchain applications in healthcare.

Qusay H. Mahmoud is a professor of software engineering in the Department of Electrical, Computer and Software Engineering at the University of Ontario Institute of Technology. His research interests include software engineering and cyber-physical systems.