Cyber security for Medical Devices Using Block chain

Dr. Karen C. Benson

Dr. Lorraine Jonassen

Dr. Binh Tran

School of Science and Technology
Georgia Gwinnett College
1000 University Center Lane
Lawrenceville, GA 30043
USA

Abstract

One only has to turn on the news each day to hear about the latest cyber security breach and escalating theft of personal information. Never in the history of data storage has information been such a valued commodity. Critics are now comparing digital theft to the bank robberies of the wild-west days. Latest among the newsworthy cyber breach incidents are the targets of biomedical devices such as pacemakers, diabetic pumps, and patient monitoring devices. The pervasiveness of smart devices, such as Android and iOS wearable technology, has created a permanent paradigm shift of data transactions in the healthcare industry. However, these connected devices have created a 'honeypot' for threat activists, making a target and a potentially grave situation for the patient. What is the best method to protect the device and the wearer? This paper endeavors to introduce the subject of blockchain as a solution to the issue of protection of biomedical devices against threats and attacks. This paper is intended to be a systematic review of the subject and an edification of block chain within the wearable medical device realm.

Keywords

Blockchain, biomedical devices, patient information protection, cyber-security in medicine, Protected Health Information (PHI), Remote Patient Monitoring, Internet of Healthy Things (IoHT), Implantable Devices, Connected Devices, Wireless Body Area Networks (WBAN), Smart Contracts, Wearable Technology

1. Introduction

One only needs to read the daily news to hear about the escalating medical cybersecurity breaches that have recently occurred in our medical system. According to the HIPAA Journal (2019), an upward trend in data breaches has occurred in the last 9 years, with the greatest number of attacks in 2015 (see Table B1). Currently, as reported by the HIPAA Journal (2019), 59% of the United States population have had their health care records breached, with data exploits being reported at more than one per day. Between 2009 and 2018, statistics show that 2,546 healthcare data breaches have occurred involving more than 500 records. These attacks include some of the giant health care providers such as Anthem, Inc., Accudoc Solutions, Inc., and Employees Retirement System of Texas. With the escalation of attacks on Personal Medical Information (PMI) comes the next iteration of cybersecurity breaches into the field of mobile platform and wearable medical devices (Clauson, Breeden, Davidson, & Mackey, 2018).

A paradigm shift in health care has moved from the doctor-centric to the patient-centric system where the patient is in direct control of their health with the use of Wireless Body Area Networks (WBANs) (Esposito, De Santis, Tortora, Chang, & Choo, 2018). The bypassing of office-visits, lost paperwork, and diagnosis delays are remedied by mobile connected devices and smart phones. Healthcare professionals and organizations concurrently agree that mobile devices improve efficiency conjointly with productivity; however, the juxtaposition is the introduction of risks in the form of data breaches and exposure of patient data (MEASURE Evaluation, 2017). Therefore, the data in-transit and at-rest must maintain data provenance; whereby, confidentiality, integrity, and availability (CIA) is paramount to a viable health network (see Figure A2).*Data provenance* can be defined as the historical record and origins of the data, i.e., the event that occurred to initiate a medical transaction (Xia, Sifah, Asamoah, Gao, Du, & Guizani, 2017).

The pervasiveness of smart devices, such as Android and iOS wearable technology, has created a permanent paradigm shift of data transactions in the healthcare industry (Esposito, et al., 2018). Given the state of medical growth and device engineering, what is the best solution to protect the patient devices and their data?

The objective of this paper is to compose a systematic literature review about patient-connected medical devices and blockchain technology as a solution to the cybersecurity issue. The method of research used is a narrative examination of the academic literature, industry and governmental statistics, with the result to explore the blockchain solution with the security of Wireless Body Area Networks (WBANs) and Protected Health Information (PHI). This perspective aims to raise awareness of opportunities for blockchain to protect technology-focused devices. In this paper, the writers investigate Remote Patient Monitoring (RPM), Internet of Healthy Things (IoHT), Implantable Devices (ID), and Wireless Body Area Networks (WBAN) and the opportunity of the Blockchain initiative in the proof-of-concept phase.

2. Historical Review

An increase in biomedical engineered devices has proliferated in the last 10 years with the advent of remote technology, Bluetooth wireless mediums, and cloud data storage (Clauson, et al., 2018). In the broader context of connected devices and mobile health (mHealth), numerous efforts to protect patient data have been undertaken by the United States (US) Health Insurance Portability and Accountability Act (HIPAA). In many instances, the development of implantable devices is a race-to-market because of both patients' demand and business profitability. For example, patients with implantable cardiac devices have become highly vulnerable due to large security holes in the software of the devices, which were designed to be remotely manipulated by the health care provider. Failure of the supply chain to produce these products in rapid deployment open the market to production in a foreign country with a potential for substandard and counterfeit devices (Clauson, et al., 2018).

Many health practitioners are listening to the public outcry to empower the patient with their own Electronic and Personal Health Records (PHR), instead of the trifecta of doctors, overpopulated medical facilities, and medical insurance companies (Griggs, Ossipova, Kohlios, Baccarini, Howson, & Hayajneh, 2018). The trend in Protected Health Information (PHI) has now enabled people of all ages to be in control of their personal health. Furthermore, with the advent of smart phones, a paradigm shift has occurred within the healthcare industry with devices which can be user-owned and installed by the healthcare provider to ensure the well-being of the wearer (Esposito, et al., 2018). Many of these devices are simply used for the gathering of information and monitoring of patients, for instance: fitness tracking, weight loss, and caloric intake. These devices function as a workout tracking tool by use of apps on the device, such as a smart phone. However, other devices have bodily embedded sensors for more advanced medical measurements such as glucose, heart rate, and epilepsy.

Digital health technologies, including mobile health (mHealth) and remote monitoring, are increasing as a practical role in medicine (Ichikawa, Kashiyama, & Ueno, 2017). mHealth has been known to lower costs by facilitating patient care and connecting people to their healthcare providers without an office visit, which propagates a faster diagnosis with beneficial results to the patient. With the use of smart phones and mobile apps, patients are empowered to proactively address medical conditions with near real-time monitoring and treatment, regardless of the locale of the patient and respective healthcare provider. With the advent of smart phone devices and the phone apps that support mobile health, there exists the potential to (a) promote improved patient outcomes in an expedient manner, (b)care coordination between multiple health care professionals, and (c)improved physician-patient communication (Ichikawa, et al., 2017).

Simultaneously, safe and accurate management of the information developed from mHealth must be established in order to return beneficial effects to both the consumer and care providers concurrently. Existing methods to effectively manage and protect the data at-rest and in-transit using implantable devices have proven ineffective or insufficient (Xia, Sifah, Asamoah, Gao, Du, & Guizani, 2017). At risk in the mobile device arena is data provenance, auditing, and medical data stored in cloud repositories. A means and method are needed to transmit patient data in a tamper-proof manner from the mobile device to the health care professional. Furthermore, there must be an implementation by which cloud service providers and other big data operatives will be able to achieve data provenance and auditing while sharing medical information for research with a collaborative diagnosis for a breakthrough discovery in curing diseases. There exists a need to share patient data between research institutions, the health care provider, and the patient (Liang, Zhao, Shetty, Liu, & Li, 2017). However, protecting the information at-rest and in-transit has become a challenge related to confidentiality, integrity, and data provenance. First, healthcare is privacy-sensitive, especially with the advent of Wireless Body Area Networks. Second, current solutions are formulated around a centralized network architecture, which is conducive to a single point of failure and requires a centralized trust system. Therefore, integrating health data into connected devices and the interoperability between healthcare provider and patient remains a constant challenge to data integrity. However, with remote patient monitoring, patients can have self -sovereignty and take control over their health maintenance with the mobile platform and wearable devices. There exists a sense of urgency to develop a user-centric access control with data privacy preservation and, yet, accessibility of the data to the healthcare provider. The user has control as to what entities are privy to the data, whether it be insurance companies or healthcare providers (Liang, et al., 2017).

The Internet of Things (IoT) is a term which describes the fact that all inordinate devices can connect to the Internet with monitoring and visual capabilities (Esposito, et al., 2018). For example, home thermostats, privacy cameras, and even washing machines can connect to the Internet for remote monitoring. A nascent subset of the IoT is the term the Internet of Healthy Things (IoHT) which describes wearable technology with the new possibilities for a patient's freedom from hospital stays, considering the advent of Wireless Body Area Networks (WBANs). WBANs have many acronyms: remote patient monitoring, implantable devices, and connected devices. All of these will record real-time measurements of a patient's vital signs, such as heart rate, glucose levels, and epileptic seizures. Many of these WBANs can provide instant treatment based on the findings of the sensors. The WBANs report back to a central location, or a master device. This master device could typically be a mobile phone or smart device, which transmits the data to the respective healthcare provider and, simultaneously, the patient. This interactive remote monitoring reduces time-consuming doctor visits and allows the patient to have great quality of life (Griggs, et al., 2018).

The momentum and possibilities of blockchain have extended from the financial sector to the health care industry since confidentiality, integrity, and authentication are significant factors in the HIPAA regulations (Angraal, Krumholz, & Schulz, 2017).In 2016, the Office of the National Coordinator for Health Information Technology organized a challenge for soliciting white papers on the potential use of blockchain in healthcare. This action started the advance in the study of how blockchain can improve Patient Health Information (PHI). Currently, blockchain assures that the digital asset exists, and the block has not been deleted or altered, rendering the data immutable.

3. Recorded Examples of WBAN Vulnerabilities

Given the purported benefits of remote patient monitoring (patient freedom, cost savings, reduced doctor visits), healthcare providers must balance the advantages with the over-encompassing cybersecurity risks (Alpine Security, 2019; MEASURE Evaluation, 2018). As medical devices become interconnected with the Internet, hospital networks, and smart phones, there exists a direct relationship between connectivity and exploits to patient data. Any device that connects wirelessly to other equipment at a central location can be compromised (United States Food & Drug Administration, 2019). Current threats range from debilitating ransomware to theft of sensitive medical records through breaching the WBANs (Alpine Security, 201). As data proliferates into the cloud data storage, hackers are drawn to the sensitivity of Protected Health Information (PHI) and with the potential of devising new tactics to gain access to the data (MEASURE Evaluation, 2017). Vulnerabilities include software, stolen devices, and data transmission channels. However, the over-arching ramification of a wearable-device breach is lack of confidence in the device when an inaccurate diagnosis is made based on the altered data.

3.1 Pacemakers

With the advent of the baby-boomer generation requiring more medical attention, remotely monitored medical devices are now in vogue with doctors and healthcare systems alike (Clauson, et al., 2018). Unfortunately, this convenience comes with a cost. With any technology that can be remotely manipulated and monitored, security attacks are inevitable without proper firmware and software updates.

On August 23, 2017, approximately 465,000 pacemaker devices were collectively recalled from Abbots (formally St. Jude Medical), by the US Food and Drug Administration (FDA) (United States Food & Drug Administration, 2019). The cardiac devices are implanted under the skin and have insulated wires that lead into the heart. A patient may need an implantable cardiac pacemaker which can mitigate a slow or irregular heartbeat. Although no equipment breach transpired, the FDA proved that a firmware update was needed for corrective action in the cardiac devices to reduce the risk of patient harm due to a potential exploitation risk. Firmware is a type of software specifically written for a certain piece of hardware, as in this case, the pacemaker software (Alpine Security, 2019).

After a thorough review, the FDA confirmed the pacemaker vulnerabilities could allow unauthorized users to access the patient's device using a common laptop (United States Food & Drug Administration, 2019). By modifying programmatic commands in the implanted pacemaker, the patient could be harmed by a rapid depletion of the battery. To address this vulnerability, the pacemaker manufacturers released a firmware update which will force any device attempting to communicate with a pacemaker to provide authorization before any actions can be performed on the device (Alpine Security, 2019). However, almost half a million users of an implantable cardiac pacemaker failed to update the device firmware, rendering the device vulnerable to a security breach. Similarly, Symbiq Infusion Systems discovered that the Hospira smart pumps could be accessed and controlled by unauthorized users to manipulate dosages to patients (Clauson, et al., 2018).

These instances are evidence to the fact that a more robust system of patient data protection is needed in the realm of implantable devices.

3.2 Drug Infusion Pumps

In September of 2017, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) determined there were vulnerabilities with the syringe infusion pumps in United States hospitals (ICS-Advisory, 2017). These infusion pumps are typically used for the delivery of insulin, hormones, antibiotics, chemotherapy, and pain relievers. Furthermore, the devices are used worldwide to deliver small doses of medication including neonatal intensive care, pediatric intensive care, and operating room procedures. The Medfusion 4000 Wireless Syringe Infusion Pump was found to have eight security vulnerabilities, including the capability for an unauthorized user to gain access and alter the intended operation of the pump. Conceivably, a threat activist could administer to the patient a fatal overdose, due to the device vulnerability. Possible device exploits included (a) improper host certificate validation in which a Man-in-the-Middle (MitM) breach could occur, (b) the use of hard coded usernames and passwords between wireless connections, abd(c) hardcoded credentials in the pump (Alpine Security, 2019).

3.3 Heart Rate Monitors

In 2008, a vulnerability in the Implantable Cardioverter Defibrillators (ICDs) was discovered by the University of Washington. These devices are implanted in the chest of heart patients to produce a concentrated electrical shock to bring the heart out of ventricular fibrillation, i.e., a heart-attack condition (Mayo Clinic, 2019). Vice President Dick Cheney was a wearer of this ICD, along with hundreds of thousands of other patients. A team of cybersecurity researchers reported they had been able to gain wireless access to the heart rate monitor and were able to deliver fatal jolts of electricity and, subsequently, shut down the device. As well, researchers reported the capability to commandeer personal patient data by eavesdropping on the wireless radio embedded in the heart rate monitor. This radio was implanted to allow doctors to monitor and adjust the device settings without surgery. The researchers stated that, currently, the risk to patients is low because an exploit would take approximately $30,000 worth of lab equipment sustained by specialists. However, the vulnerability suggests too little attention is being given to cybersecurity in the escalating number of medical wearable devices equipped with wireless communication capabilities (Alpine Security, 2019).

These examples illustrate the challenges of the Internet of Healthy Things (IoHT) and how early development and adoption can many times outpace security requirements and proper testing procedures. In response to public outcry, government and regulatory agencies are moving to increase awareness with the health community concerning the risks of these IoHT devices (Esposito, et al., 2018).

4. Solutions Provided by Blockchain

What is the common denominator that would provide confidentiality, integrity, and accessibility for connected devices? All of the more critical challenges could be addressed by blockchain technology (Clauson, et al., 2018). Just as the Internet was a great paradigm shift in business, research/development, and medicine, blockchain is a new architype, where applications of this discovery are being developed daily (Griggs, et al., 2018). This paradigm shift will replace the old standards and traditions with new use cases. Blockchain is poised to alter the digital world, not unlike emergence of the World Wide Web 25 years ago (Booker, 2018).

Is blockchain the panacea for Healthcare and wearable devices? By its definition, blockchain is a distributed, decentralized, and immutable ledger where the middleman is eliminated (Brown, 2018) (see Figure A2). As stated byXia et al. (2017), blockchain can be visualized as a virtual ledger, or database, that houses a sequential list of records linked together in blocks which contain information about a particular transaction. This growing list of records or blocks are considered immutable, as each block is replicated in a peer-to-peer network. This immutability principle is the cornerstone of the security in blockchain, making it a recognized solution to achieve a secured distribution of medical information in an untrusted realm. The main function of the blockchain network is to uphold a chronologically, distributed, and immutable database of transactions (Angraal, et al., 2017).

Made popular by the success of the virtual currency of Bitcoin, blockchainis the under-pinning of Bitcoin, and can also be used in other paradigms. Originally, blockchain was designed in 2008 as a mechanism to transport and verify the Bitcoin technology, a virtual currency which is not traceable (Griggs, et al., 2018). Despite the meteoric rise of Bitcoin, it is not appropriate in the medical field for three reasons (a) Bitcoin in is an open network which any user can join,(b) Bitcoin only deals with currency and not medical records,and (c) Bitcoin uses massive resources to guarantee a tamper resistant blockchain. However, the underlying blockchain technology is very suitable for building cryptographic proof of medical systems and tamper-resistant medical mobile devices (Ichikawa, Kashiyama, & Ueno, 2017). The same ability that Bitcoin imbued in blockchain is the requisite for blockchain to broadcast transactions over a peer connected network, which proves vital for the privatization of other types of transactions (Angraal, et al., 2017).

The general public may confuse cryptocurrencies and blockchain, since both arrived on the virtual scene at the same time (Brown, 2018). However, the two can be split apart, making blockchain useful for many other purposes. The concept of blockchain had its origins in 1991, when researchers were attempting to timestamp digital documents to avoid backdating and tampering with evidence (Angraal, 2017; Decuyper, 2017). In 2009, this timestamping was discovered by Satoshi Nakamoto, who used the concept in Bitcoin, or today's cryptocurrency. The blockchain concept has evolved for other uses such as voting, legal documents, and medical records. In its basic concept, blockchain is a technology that is able to construct a distributed online database consisting of blocks that are linked with each other (Esposito, 2018; Decuyper, 2017). Each transaction, typically from a smart phone device, is represented in a cryptographically signed block and is replicated in a peer-to-peer format throughout the blockchain (Angraal, et al., 2017; Ichikawa, Kashiyama, & Ueno, 2017).

Blockchain is considered as an immutable, distributed ledger, meaning the blocks cannot change or be deleted (Decuyper, 2017). The word 'immutability' is a key property of the blockchain principle and is a practical difference compared with the traditional debit and credit transaction processing (Angraal, et al., 2017). As well, the blocks are replicated in a peer-to-peer fashion (Decuyper, 2017). The content of the block may vary; however, each block will contain: 1) data, 2) hash of the blockchain, and 3) hash of the previous block. The data in a health care blockchain will contain transaction information. Other types of blockchains will contain differing types of information, such as Bitcoin transactions. The hash of the block is analogous to a fingerprint. Each person has a unique fingerprint, as does the hash of a block. Changing the data inside the block will change the hash of the block, which signifies the block has been tampered with. The third element inside of a block is the hash of the previous blockchain; thereby, linking the blocks in the chain together. This hash chaining is one reason why the blockchain is considered a secure mechanism for secure healthcare transactions (Decuyper, 2017 (see Figure A3).

The second security characteristic of blockchain is the distributed mechanism, or a peer-to-peer network, in which there is no single point of failure (Angraal, et al., 2017). These peer-to-peer nodes are called *miners* and are considered the 'keepers of the blockchain' with a full copy of the blockchain. A miner is a person or entity who validates the blockchain and the transactions as they are added. Miners have no qualifications and can be anyone who desires to invest large capital resources required to be a miner of the blockchain, as the software is open-source and free to download. In return, these miners are paid in the form of Bitcoins for every block of transactions they add to the blockchain. Each miner verifies that all blocks are in order by comparing his blocks with other miner's blocks (Angraal, et al., 2017; Decuyper, 2017). When a new block is created, every miner in the blockchain receives a copy of the same block. Hence, in order to successfully tamper with the blockchain, a threat activist must re-construct all the blocks in the blockchain.

There exist three types of blockchains: public, private, and consortium (which is a combination of the two) (Griggs, et al., 2018). A public blockchain is analogous to the Internet, in which all parties participate in the conversation of the World Wide Web. Conversely, a private and semi-private blockchain are analogous to a company Intranet, where information is disseminated to those who have a particular interest in the data. In the latter, more control and privacy are provided over who can view the information. In the case of PHI, the key reason for using blockchain is to decrease costs and increase privacy for PHI. This is accomplished by decentralization of the information and a virtualized general ledger for all transactions. Once information is entered into the blockchain, the block within the chain cannot be deleted or altered; effectively, the block is immutable. Similar use cases include logistics (transportation of goods), originality of artwork, and even as ordinary as the authenticity of organic produce. In this situation of blockchain PHI, confidential medical information will not be stored because of HIPAA compliance regulations. The blockchain will be a technology ledger, recording the events as they occur on the front end. On the back end, patient statistical measurements will be forwarded to a designated Electronic Healthcare record (EHR) database, and the blockchain will record a successful data processing (Griggs, et al., 2018).

Esposito, et al. (2018) delineated the advantages of blockchain in the medical industry as such:

- There is no middleman, or mediator, which avoids the bottleneck and single point of failure.
- Patients have control over their data, with the capability to determine who can read the healthcare information in the blockchain.
- The medical data history in the blockchain is consistent, immutable, accurate, and distributed to multiple nodes for authentication.
- Addition of blocks to the blockchain are visible to members whom the patient has allowed to view. Any unauthorized modifications can be detected by the different nodes and disallowed to add to the blockchain.

It is evident from these blockchain principles that technology can play a significant role in enhancing the independence of a patient from being tethered to a monitoring device at a brick-and-mortar institution (Esposito, et al., 2018).

With the tamper resistant mHealth system of blockchain, the manipulation of data stored in servers is rendered nonexistent (Ichikawa, et al., 2017). Through blockchain, there exists an application that gives patients the ability to grant access of medical records and information to designated caregivers and other institutions, thus, making the current medical records system a patient-centric approach (Griggs, et al., 2018).

As a secondary advantage, data analytics can be leveraged to make more informed medical decisions for the patient. By using this new technology paradigm, cost reduction will be realized in terms of personnel, equipment, and infrastructures necessary to treat patients (Griggs, et al., 2018). Furthermore, the need for data sharing in real-time healthcare situations between different providers and across nations has become more pronounced. The following table exemplifies the differences between the traditional PHI system and the blockchain system.

	Traditional System	**Blockchain**
Confidentiality	Encrypted data end-to-end.	Encrypted data end-to-end.
Availability	Uses database and archaic backup systems. Single point of failure.	All nodes have a copy of the blockchain with every recorded transaction providing redundancy.
Integrity	Databases are vulnerable to both threat activists and accidental manipulation.	The blockchain is immutable. Blocks cannot be change or deleted.
Traceability	Consistency of health records are not guaranteed.	Blockchain transactions are replicated in a peer-to-peer fashion. All blocks can be traced from origin of creation and are immutable.
Speed	Transactions are limited by the speed of the local network.	A negligible delay may occur due to the building and adding of another block to the chain.
Privacy	Transactions can be traced back to the end user even with end-to-end encryption.	Anonymous addresses will protect the identity of patients.
Transparency	Patients do not have control over their own PHI records and cannot remotely view their records.	Patients can link into their blocks on the blockchain and remain in control of their information.

Note: Table detailing the differences between the traditional PHI system and the blockchain system (Griggs, et al., 2018).

5. Smart Contracts

To accommodate (PHI) Griggs, et al. (2018), recommended using blockchain based smart contracts which would create data analysis and management of the devices connected to sensors. The authors devised a system where the sensors in the implantable device communicate with a smart device, such as a cell phone or tablet. Subsequently, the smart device calls and communicates to a smart contract where the data is transferred to the blockchain. Using this method, the blockchain would communicate real-time patient monitoring by sending pertinent information and medical intervention notifications to the appropriate medical professionals and patients in a HIPAA compliant manner (see Figure A4).

The term, smart contracts, was first used by Nick Szabo in 1997, before the creation of Bitcoin, as a mechanism to store legal contracts (Decuyper, 2017). Smart contracts are analogous to legal written contracts, with the exception that they are completely digital and do not require a 3rd party for implementation. The smart contracts consist of a computer program stored inside a blockchain. These simple programs can be used to automatically exchange data based on certain conditions. Because the smart contracts are stored inside blockchain, they inherit the security properties of the blockchain, such as immutability and peer-to-peer distribution.

Ichikawa, et al. (2017) described smart contracts as a function that will be executed when prompted by an action. For instance, when a smart phone has collected a certain amount of data on an insulin pump, the data will be passed to the smart contract. The purpose of a smart contract is to identify certain actions that must be performed on data from the smart phone. Again, in this example, the smart contract knows that this patient's insulin level should always be at 100 (for example), and the patient may need more insulin at this time. To address the concerns of HIPAA compliance, physicians, and patients, Griggs, et al. (2018) has suggested using smart contracts in conjunction with block chain.

This method will provide a distributed data processing service combined with an immutable log of the transactions between the remote devices and healthcare providers. For privacy, verifiability, and authenticity, blockchain uses a distributed ledger allowing only authorized entities to examine the blockchain for verification. This 'medical ledger' would be unchangeable, and incontrovertible, giving real-time notification of health events in a secure manner to the health provider and the patient wearing the medical device. Thus, the practice of precision medicine in an instantaneous manner would benefit the medical system as a whole. Furthermore, with the use of blockchain, crowd sourcing of medical diagnosis and information could be used for diagnostic purposes in similar cases around the world. Concurrently, the patient would have their own anonymous account that could be traced only at their discretion.

Due to HIPAA compliance regulations, no confidential medical information concerning patients will be stored in the blockchain or on the smart contracts. The reasoning is two-fold. First, the blockchain is not designed to hold large amounts of data. Second, HIPAA compliance will not allow PHI to be stored in the blockchain. Using the blockchain ledger system, the patient transaction serves as a separate form of security for both the caregiver and the patient. A further benefit of blockchain is that it provides immutable record keeping and patient authenticated monitoring which can be used for settling disputes or any medical investigation (Griggs, et al., 2018).

6. Limitations of Blockchain

The greatest advantage and feature of blockchain exists as the immutability principal that any data added to the blockchain cannot be deleted or altered. However, all data of a personal nature comes under the soon-to-be-enforced, General Data Protection Regulation, which states the right-to-erasure for individuals. This presents a problem given the immutability principal of blockchain (Esposito, et al., 2018).

On a practical side, how robust is blockchain in its ability to store voluminous healthcare data? Blockchain, in its originality, was promulgated to store small pieces of Bitcoin transaction data. Healthcare data, such as imaging and lab results, can be gigabit intensive, which can slow the real-time effectiveness of data transmission. In an effort to mitigate these issues many have suggested storing the data outside of blockchain and storing the hash of the health data in the blockchain. This would effectively sustain the advantages of both worlds. The future holds the answer as right-to-privacy litigators continue to regard personal data as owner-specific, whether the information is in a hash format or in clear text. This means the patient must be able to change or delete any health data whether in hash format or clear text (Esposito, et al., 2018).

Several possible limitations exist in comparison with traditional data storage versus blockchain (Angraal, et al., 2017). First is the scaling of blockchain, and the cost effectiveness of implementing blockchain into the medical field. This potential issue would need to be addressed, particularly, with emergency remote patient monitoring. The second consideration is the outlay of expenditures for hardware, system implementation, and training which would need to be determined for the return on investment to be realized. These limitations create an argument as to the inverse relationship in providing transparency and authenticity to the data transactions while incurring the cost to deploy blockchain. Based on these limitations, Blockchain may not yet be the panacea for medical device data transmission. Nevertheless, a peer-to-peer system that eliminates an intermediary (single point of failure) has a substantial potential in creating confidentiality, authenticity, and integrity in connected devices and remote patient monitoring.

Several potential barriers prohibit the entire health record being placed in the Blockchain. First, the blockchain must be in compliance with regulatory requirements of HIPAA. Second, technical barriers exist related to data storage and distribution of information. Therefore, most proposals of blockchain in healthcare focus on privacy of data, auditing, data provenance, and authorization (Angraal, 2017). Furthermore, under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), it should be noted that blockchain is not covered under the current rule system, since each block cannot be identified as belonging to a specific patient (Griggs, et al., 2018). As previously noted, the blockchain contains information about many patients; therefore, the blockchain will relay information about a particular transaction from the host to the database and not sensitive health data specifically. Not unique to blockchain, the greatest challenge in healthcare is maintaining end-to-end security from the smart device to the database. Many smart devices transmit data over a private WIFI, such as a home network. Concurrently, data may be sent by the patient using a public WIFI, for instance, a coffee shop. In either case the data must be encrypted for end-to-end security. A key aspect of healthcare is the speed in which data is transferred in real-time. Blockchain times may introduce some minor delay, which may affect emergency decisions by the caregiver and patient. Therefore, the blockchain system may not be a preferred method for emergency response due to the previously stated constraint. Many of the blockchain limitations may be overcome with future developments relating to remote patient monitoring (Griggs, et al., 2018).

7. Conclusion

In 2016, 7.1 million patients in the world utilized some facet of remote monitoring as a part of their health management system (Griggs, et al., 2018). As baby-boomers age, it is predicted that by 2021, 50.2 million will be joining the realm of implantable and connected devices, especially with the Medicare and Medicaid Services giving reimbursement incentives. Furthermore, healthcare data is considered a 'honeypot' for malfeasants and threat activists. For instance, threat activists may seek financial gain from data theft to sell to a third-party, who may be interested in DNA issues and pre-existing conditions of a patient. These episodes have motivated the government to regulate insecure protected health information (PHI) transmission (Esposito, et al., 2018). Patient privacy and electronic health records (EHR) must be preserved as per HIPAA regulations, despite the many different sensor devices made by varying manufacturers and differing standards of protection. Additionally, patients must permit what data will be of record to the attending physician and what type of timeline of events the patient desires (Griggs, et al., 2018).

This paper was not meant to ascertain the efficacy of block chain but to introduce medical professionals to the concept of security with bio-medical devices using block chain. As there exists a preponderance of advanced research topics concerning block chain, the intent of these writers was to focus on the current threat against medical devices and the protection thereof. These authors believe that by exposing the current threats, more medical personnel will embrace and adopt the block chain solution for protection of medical devices and, hence, the protection of the patient. Paramount is the necessity of medical professionals to comprehend the basic principles of block chain and use the information to advance this topic into the medical field. This goal is accomplished through a detailed level of understanding by the biomedical engineer and the medical professionals, with a subsequent outcome of a categorical teaching method to a greater audience of professionals in the medical field.

References

Alpine Security. (2019). *Most dangerous hacked medical devices.* Retrieved from https://www.alpinesecurity.com/blog/most-dangerous-hacked-medical-devices

Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology: applications in health care. *Circulation: Cardiovascular quality and outcomes*, *10*(9). doi.org/10.1161/CIRCOUTCOMES.117.003800

Bheemaiah, K. (2015). *Why business schools need to teach about the Blockchain: An overview of Cryptocurrency and Blockchain technology based on business initiatives and models.* Retrieved from SSRN: https://ssrn.com/abstract=2596465

Booker, E. (2018). Blockchain, bitcoin, & Beyond. *GTalumni.org, 94*(2), 61-65. Retrieved from https://www.gtalumni.org/s/1481/alumni/17/magazine-pages.aspx?pgid=14273&gid=21&cid=32290

Clauson, K., Breeden, E., Davidson, C., & Mackey, T. (2018). Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: An exploration of challenges and opportunities ini the health supply chain. *Blockchain in Healthcare Today*, *1*. doi.org/10.30953/bhty.v1.

Decuyper, X. [Savjee]. (November 13, 2017). *How does a blockchain work – Simply Explained* [Video file]. Retrieved from https://www.youtube.com/watch?v=SSo_EIwHSd4

Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy?. *IEEE Cloud Computing*, *5*(1), 31-37. Retrieved from https://pdfs.semanticscholar.org/7f8f/4ff1377ebf0a084c44dbf6926af03dd2cdd8.pdf

Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of Internet of Things (IoT). *International Journal of Computer Applications*, *111*(7), 1-6. Retrieved from https://pdfs.semanticscholar.org/35f0/899d941e9e34ff1225448c21662d5ccca74c.pdf

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). doi.org/10.007/s10916-018-0982-x.

HIPAA Journal. (2019). Healthcare Data Breach Statistics. Retrieved from https://www.hipaajournal.com/healthcare-data-breach-statistics/

Ichikawa, D., Kashiyama, M., & Ueno, T. (2017). Tamper-resistant mobile health using blockchain technology. JMIR mHealth and uHealth, 5(7). doi.org/10.1161/CIRCOUTCOMES.117.003800

ICS-Advisory. (2017). *Smiths Medical Medfusion 4000 wireless syringe infusion pump vulnerabilities* (Update A). CSMA-17-250-02A. Retrieved from https://www.us-cert.gov/ics/advisories/ICSMA-17-250-02A

Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (pp. 1-5). IEEE.doi: 10.1109/PIMRC.2017.8292361

Mayo Clinic. (2019). *Implantable cardioverter-defibrilators (ICDs).* Retrieved from https://www.mayoclinic.org/tests-procedures/implantable-cardioverter-defibrillators/about/pac-20384692

MEASURE Evaluation. (2017). *Improving data quality in mobile community-based health information systems—Guidelines for design and implementation*. Chapel Hill, NC, USA: MEASURE Evaluation, University of North Carolina. Retrieved from https://www.measureevaluation.org/resources/publications/tr-17-182.

United States Food & Drug Administration. (2019). Firmware update to address cybersecurity vulnerabilities identified in Abbot's (formerly St. Jude Medical's) implantable cardiac pacemakers: FDA safety communication. Retrieved from https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals

Walport, M. (2016). Distributed ledger technology: Beyond blockchain. *UK Government Office for Science.* Retrieved fromhttps://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Xia, Q. I., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access, 5,* 14757-14767. doi: 10.1109/ACCESS.2017.2730843

Appendix A: Figures

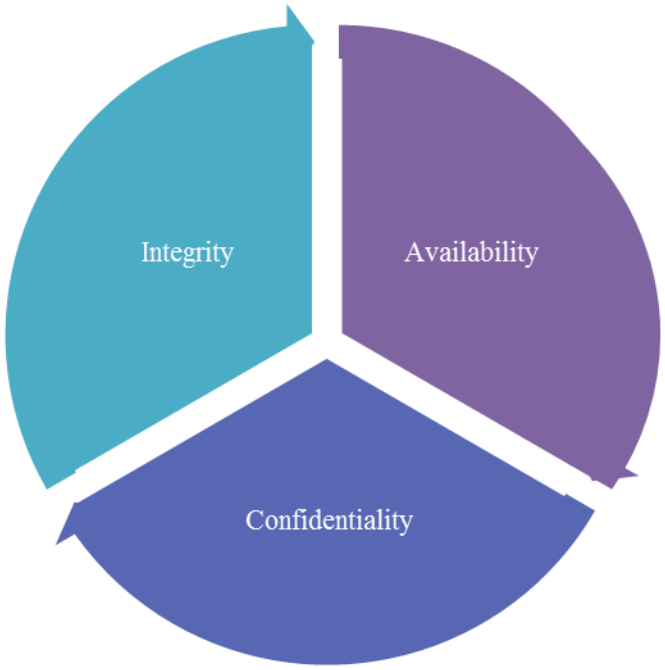


Figure A1. Confidentiality, Integrity, and Availability (CIA) Triad depicting the ability of blockchain to provide information within these parameters. In a client-server network topology, such as a medical office with a server, a breach in any of the three areas would mean a single point of failure for patient data. Confidentiality is the absence of external interference, such as ransomware. Integrity is the absence of data alteration including protection against cyber malfeasants. Availability is the assurance that information and data are readily available, especially in the case of connected medical devices (Source: Farooq, Waseem, Khairi, & Mazhar, 2015).

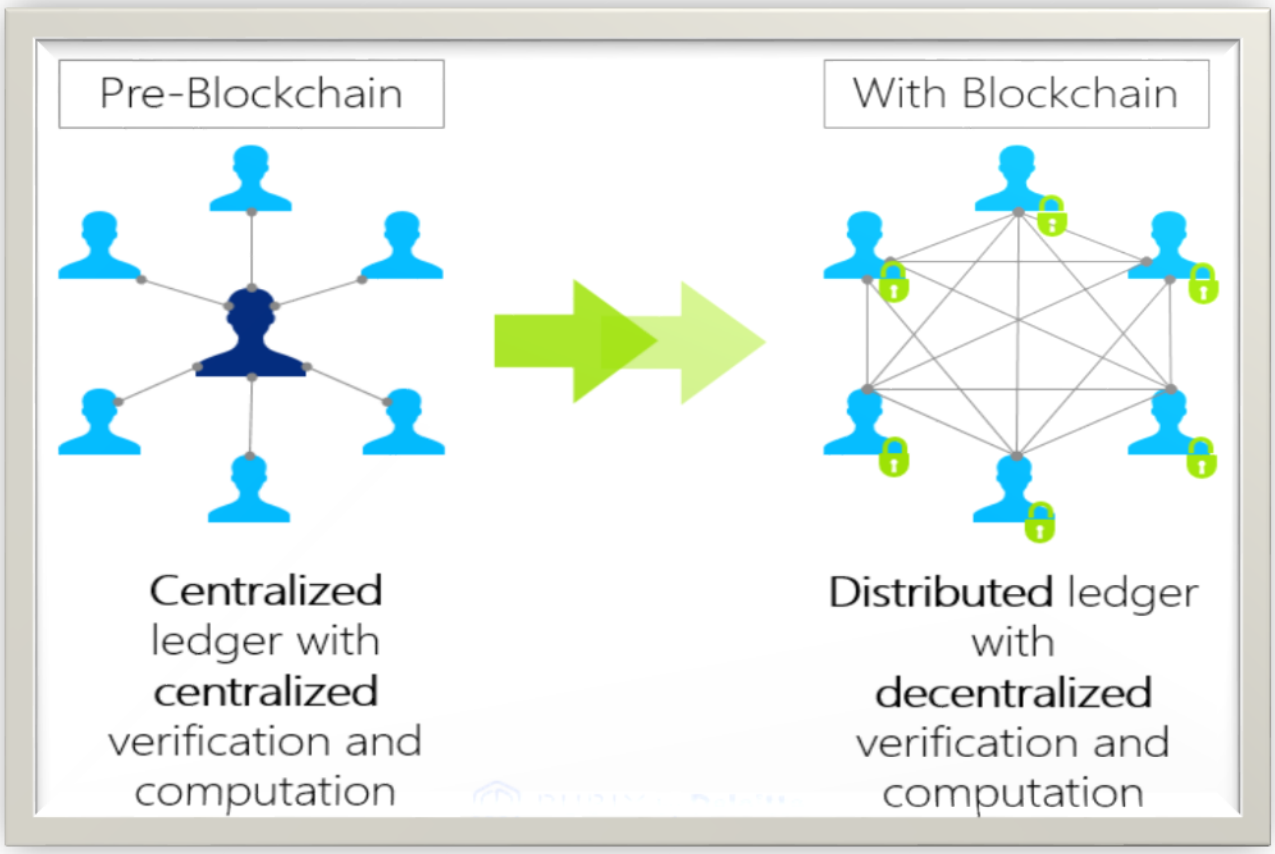


Figure A2. A figure depicting a decentralized network topology.In this example, no centralized server of medical information exists. Therefore, the single-point-of-failure problem is non-existent as in the case of ransomware attacks on servers. In the blockchain, all nodes replicate within the network assuring data provenance, as well as, confidentiality, availability, and integrity (Source: Walport, 2016).

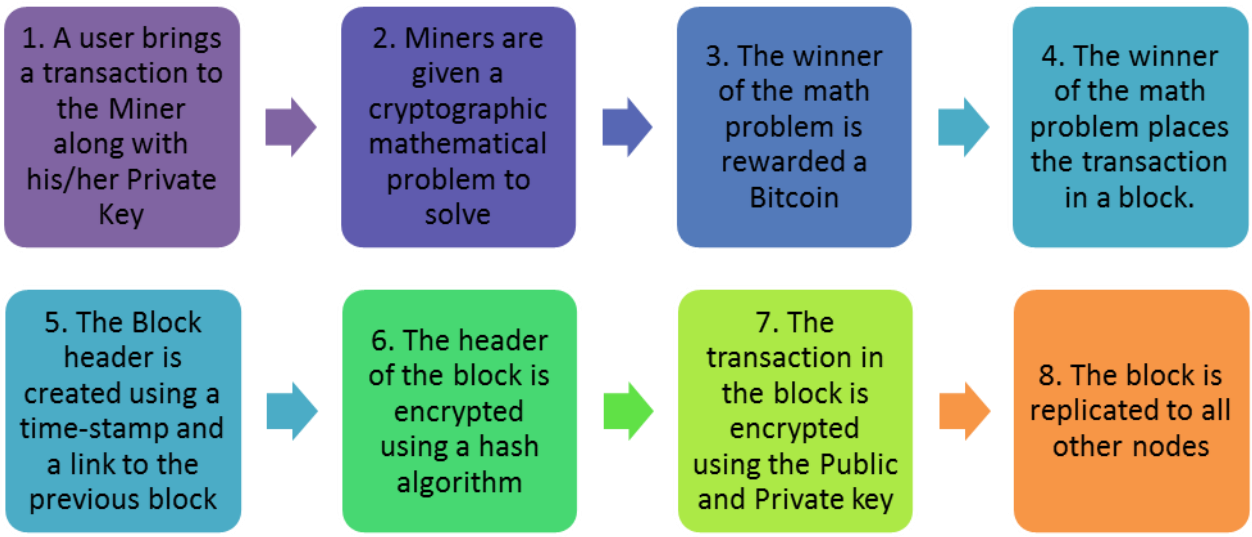


Figure A3. Depicting the asynchronous steps to add a block to the blockchain (Source: Bheemaiah, 2015; Dack & Letten, 2018).

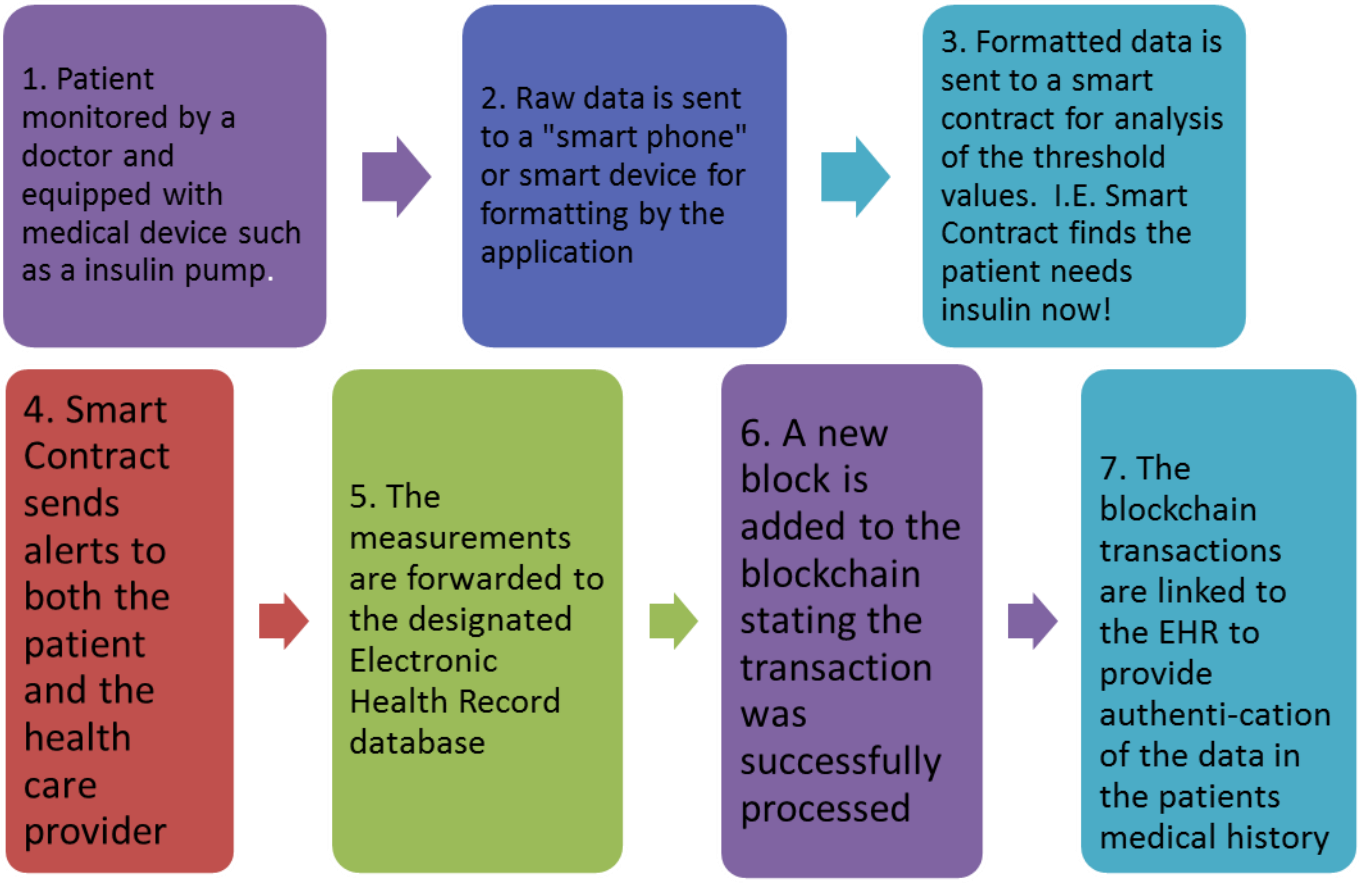
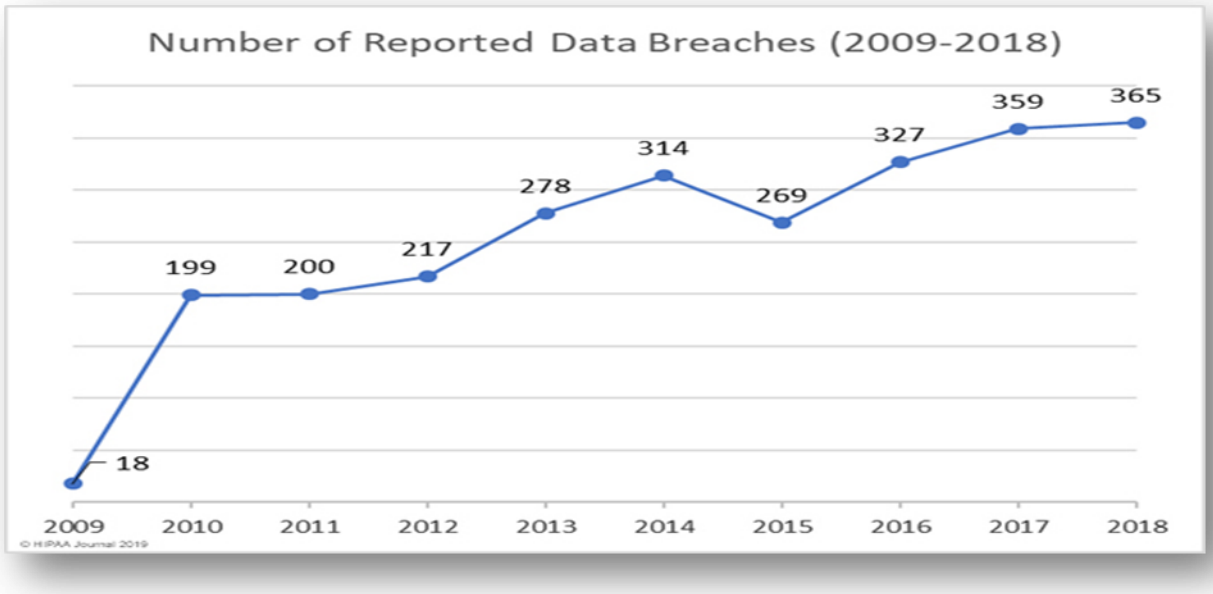


Figure A4. Depicting the steps to add a smart contract to the blockchain (Source: Decuyper, 2017; Griggs, et al., 2018; Ichikawa, et al., 2017).

Appendix B: Tables
Table B1
Medical Breaches by Year



Note. Showing the Medical Records breaches from 2009-2018. (HIPAA Journal, 2019).