Accepted Manuscript

Blockchain in healthcare applications: Research challenges and opportunities

Thomas McGhin, Kim-Kwang Raymond Choo, Charles Zhechao Liu, Debiao He

PII: S1084-8045(19)30086-4

DOI: https://doi.org/10.1016/j.jnca.2019.02.027

Reference: YJNCA 2331

To appear in: *Journal of Network and Computer Applications*

Received Date: 1 September 2018

Revised Date: 30 January 2019

Accepted Date: 25 February 2019

Please cite this article as: McGhin, T., Raymond Choo, K.-K., Liu, C.Z., He, D., Blockchain in healthcare applications: Research challenges and opportunities, *Journal of Network and Computer Applications* (2019), doi: https://doi.org/10.1016/j.jnca.2019.02.027.

Blockchain in Healthcare Applications: Research Challenges and Opportunities

Thomas McGhin[1], Kim-Kwang Raymond Choo[1], Charles Zhechao Liu[1], Debiao He[2]

[1] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA
mcghin.thomas@gmail.com, raymond.choo@fulbrightmail.org, Charles.Liu@utsa.edu

[2] Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan, China and the State Key Laboratory of Cryptology, Beijing, China
hedebiao@163.com

Abstract: **Blockchain has a range of built-in features, such as distributed ledger, decentralized storage, authentication, security, and immutability, and has moved beyond hype to practical applications in industry sectors such as Healthecare. Blockchain applications in the healthcare sector generally require a greater level of authentication, interoperability, and record sharing due to exacting legal requirements, such as Health Insurance Portability and Accountability Act of 1996 (HIPAA). Building on the existing blockchain technology, researchers in both academia and industry have started to explore applications that are geared toward healthcare use. These applications include smart contracts, fraud detection, and identity verification. Even with these improvements, there are still concerns as blockchain technology has its own specific vulnerabilities and issues that need to be addressed, such as mining incentives, mining attacks, and key management. Additionally, many of the healthcare applications have unique requirements that are not addressed by many of the blockchain experiments being explored, as highlighted in this survey paper. A number of potential research opportunities are also discussed in this paper.**

Keywords: Blockchain, Healthcare Industry, Authentication, IoT, Wireless, Vulnerabilities, Survey

1. INTRODUCTION

Blockchain is a technology and architecture platform that was launched in 2009 [1]. Blockchain works by storing information in recording ledgers that are distributed in a decentralized manner across all computing devices that are part of the blockchain infrastructure [1]. The infrastructure is peer-to-peer based and functions by having both users of the network that participate in transactions and the blockchain miners that facilitate the transactions in a distributed ledger. The ledger is stored in a decentralized network of nodes that are created through cryptographic processes computed by all miners within the network [2]. In addition, the blockchain ledger offers highly reliable storage capabilities as it is creating using consensus mechanisms, digital signatures, and hash chains [2]. Due to these advanced features, Blockchain provides numerous services including traceability, integrity, security, and non-repudiation while storing all information in a public decentralized manner, while maintaining privacy [2].

Blockchain has applications in sectors such as banking, finance, real estate, and government [3-5]. While banking and finance have had more research dedicated to them, healthcare only recently started to receive more attention on blockchain enabled applications [4, 6-9]. A number of researchers have highlighted the potential of using blockchain technology to address existing challenges in healthcare applications [4, 6-9] [2, 10-30], which is the focus of this literature review. For example, Cheng et al. [72] explored the potential of using blockchain to link patients' electronic health records across the different healthcare services in China.

In this literature review, we survey published literature to understand the current state of research relating to the potential of blockchain applications in healthcare. We search for the publications on Google Scholar using keywords such as the following:

- Blockchain AND healthcare AND (site:sciencedirect.com OR site:ieee.org OR site:springer.com OR site:dl.acm.org OR site:journals.sagepug.com OR site:tandfonline.com OR site:plos.org)[1]

The term healthcare was chosen as a means to target only the articles that were relevant to this literature review. Other terms were considered (such as medical), but did not give papers that met the criteria sought out for this literature review. An established protocol from primsa-statement.org was adopted to evaluate and select the research material to be included in this literature review. The protocol provides various criteria and detailed guidance on how the citations can be used and how a specific research work should be included or excluded [37]. In addition to the protocol, additional inclusion and exclusion criteria were employed based on the significance of the topic and the freqency Blockchain, Healthcare, or both were referenced in the research. Articles were manually excluded if they only mentioned the topic once or only used the word Blockchain and Healthcare out of context. Using these methods the number of articles was reduced to the 69 referenced for this literature review.

To explore the literature related to blockchain, we located seven existing surveys on blockchain covering different perspectives and summarize these studies in Table 1. For example, in [31], the authors conducted a systematic examination of the security from a variety of threat actors against the blockchain system. Tschorsch and Scheuermann [32] surveyed all digital currencies that have been in development since the inception of Bitcoin and Blockchain. Conoscenti, Vetro, and De Martin [33] examined the peer-to-peer architecture of blockchain and its applications to Internet of Things (IoT). Karafiloski and Mishev [34] surveyed big data and IoT applications for blockchain. Sankar, Sindhu, and Sethumadhavan [35] conducted a systematic review of a variety of emerging consensus protocols that will help move blockchain technology forward toward a Byzantine fault tolerant consensus protocol that is global and allows cross-platform plug and play software applications [35]. In the survey of Zheng, et al. [1], they presented an overview of the blockchain architecture, consensus algorithms, and technical challenges and advances. Rather than focusing only on Bitcoins, the survey of Mukhopadhyay, et al. [36] focused on other popular cryptocurrency systems [36].

In the next section, we will introduce unique healthcare related issues and problems facing the industry, followed by the blockchain technology and its unique features and applications that can be directed to solve the healthcare challenges in Section III. In Section IV, we will review existing literature dedicated to blockchain applications in the heathcare arena. The last section is a discussion of the merit of blockchain related technology applied to the healthcare field, with a conclusion focusing on the gaps in research and future work to be conducted.

Survey context	**Survey period**	**Number of articles surveyed**	**Literature review protocol / approach used, if any?**	**References**	**Published**
A Survey on the Security of Blockchain Systems	2006 – May 2017	71	None	[1]	2017
Decentralized Digital Currencies	2008 - 2017	243	None	[2]	2016
Blockchain for the Internet of Things	Not specifically mentioned	35	Whitelist Approach	[3]	2016
Blockchain Solutions for Big Data Challenges	2008-2016	27	None	[4]	2016

[1] In other words, we are taking a white-list approach to focus only on publications appearing in https://www.sciencedirect.com/, https://ieeexplore.ieee.org/Xplore/home.jsp, https://link.springer.com/, https://dl.acm.org/, https://journals.sagepub.com/, https://www.tandfonline.com/ or https://www.plos.org/.

Survey of Consensus Protocols on Blockchain Applications	2008-2016	15	None	[5]	2017
An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends	1997-2016	54	None	[6]	2017
A Brief Survey of Cryptocurrency Systems	1989 - 2015	69	None	[7]	2017
Blockchain versus Database: A Critical Analysis	2013 - 2018	Sample of 100 papers	None	[70]	2018
Survey on blockchain for Internet of Things	Not specifically mentioned	244	None	[71]	2019
A Systematic Literature Review of Blockchain Cyber Security	All available papers to 2018	72	Whitelist Approach	[73]	2019

Table 1 – Example of existing blockchain literature surveys relating to healthcare

2. HEALTHCARE INDUSTRY

Healthcare as an industry has unique requirements associated with security and privacy due to additional legal requirements to protect patients' medical information. In the Internet age where sharing of records and data becomes more prevalent with cloud storage and the adoption of mobile health devices, so too does the risk of malicious attacks and the risk of private information being compromised as it is shared. As health information is becoming more easily to obtain through smart devices, and patients are traveling to multiple doctors, the sharing and privacy of this information are a concern. The unique requirements the healthcare industry is facing are in the form of authentication, interoperability, data sharing, the transfer of medical records, and considerations for mobile health. Each of these requirements is described below – see also Table 2.

Requirements	**Topics**	**References**
Security	Access Controls, Authentication, non-repudiation, and interoperability	[2, 4, 6, 9, 11, 19, 30, 33, 45, 48, 59, 50, 51, 53, 54, 48, 63]
Interoperability	Centralized Data Storage	[25, 37-39, 54]

Data Sharing	Data Sharing and Access	[16, 35, 52]
Mobility	Mobile Health	[53]
	Security in the IOT Heathcare Applications	[2, 3, 14-16, 18, 24, 29, 42, 54, 57-64]
	Wireless Security Threats	[13, 51, 52, 54, 56, 58, 59, 64]

Table 2 – Healthcare Issues

2.1 System Security

As previously discussed, access controls, authentication, non-repudiation of records are major security requirements associated with healthcare and medical data, for example in ensuring integrity, confidentiality, and availability of medical information [7,8, 9, 48, 49, 50]. Medical information can be both medical records such as patient files as well as medical data that is retrieved from body sensors and other applications. As medical records are being transferred from paper to digital mediums, it requires additional security and role based privileges to be put in place to protect information and security of the healthcare records. For example, with healthcare records being stored in databases, only authorized individuals should be able to access those records and such access needs to be enforced and monitored. Healthcare records and queries to access those records require auditing of the query and strict access controls to minimize the risk of tampering or copying of those records [21].

In addition, the encryption of medical records (e.g. electronic health records – EHR, EMR, and personal health record – PHR) can be problematic if different encryption standards are used in different systems [40, 48, 50, 52]. In other words, interoperability issues – see also Section 2.2.

Current methods to protect and secure records have proven not to be as efficient as they should be, and dissemination of a patient's medical records can have real-world consequences (e.g. risks to patients' privacy in the form of malicious attacks, which can damage the reputation and finances related to those records) [19, 40].

2.2 Interoperability

Interoperability is also a major requirement for the healthcare industry. Interoperability is the process of sharing and transferring data among different sources [11]. The main limitation stopping interoperability is the use of centralized data storage in medical institutions. Centralized data storage is an issue for healthcare providers as they store all records in one central database or databank. The specific issues that arise from centralized data storage are fragmentation of health data, slow access to medical data, the lack of system interoperability, patient agency, data quality, and quantity for medical research [11]. Many records are generated daily and are stored in a centralized location at different hospitals [50]. Records that are scattered in various hospitals can be lost and the data contained will not be able to be accessed by the patient [11]. Many records end up fragmented due to the centralized nature of the health record storing system [17] [50, 51]. Centralized data authorities are needed to ensure a reliable database in an untrusted network [20].

2.3 Data Sharing

Data sharing and access is both a security problem and an inherent problem with civilian health records [10]. Healthcare record sharing is sometimes difficult as an individual's comprehensive records can be stored through a variety of locations [10]. Patients do not have a unified view of these scattered records and this applies to healthcare providers, as they do not have access to up-to-date data regarding the patients if the records are located elsewhere [10]. Healthcare records are distributed among different hospitals making sharing difficult as there is a gap is record linkage that is the concept of joining datasets based on entities that may or may not share a common identifier, such as social security number [50]. A main problem with data sharing is interoperability (see Section 3.2) [11, 51].

2.4 Mobility

Mobility is a growing requirement in the Healthcare industry as patients become more mobile and demand their records meet the same level of portability. As smart devices, sensors, and other internet enabled devices become more prevelant, the ability to transport that data is also important. In addition, the need to have real-time sharing and access to data from anywhere on any device compounds the challenge of ensuring data are secure and

protected as mandated by the law. The concept of mobility is broken into three main sections for the purposes of this paper: Mobile Health, Wireless, and IoT.

2.4.1 MOBILE HEALTH

Mobile Health (mHealth) is a growing field in healthcare applications involving devices such as miniaturized sensors, low-power body-area wireless networks, and pervasive smartphones [53]. mHealth suffers from many of the problems that the broad healthcare centralized server systems suffer. The specific problems are data sharing and consent management, access control, authentication, and user trust [53, 54]. Achieving privacy and security in a wireless sensor network (WSN) or IoT takes extensive resources, but mismanaged and compromised healthcare information can 'hurt' the patient and the future prospects of mobile heathcare applications [54]. These threats emerge as healthcare organizations that use the technology may not have the expertise to adequately secure the patient data [53]. In addition, devices can be lost or connect to an unencrypted network can result in malware or other malicious attacks [52].

Wearable technology is another technology that has healthcare applications with potential security implications. Specific privacy concerns arise from wearable technology in the form of health information sensitivity and legislative protection [60]. Sensors, devices, and smart technology have privacy concerns in the form of information disclosure, withholding information or services, modification of information, repudiation, non-auditability, and loss of authenticity / validity [61].

2.4.2 WIRELESS

A Wireless Body Area Network (WBAN) deployment can include wearable body sensors [56] [57], and related security threats include data integrity, data freshness, availability of the network, data authentication, secure management, dependability, secure localization, accountability, and flexibility [56, 57]. Devices in a WBAN are also likely to be resource constrained [13], and hence lightweight security solutions will be required.

Additional problems associated with wearable health technology are that the data can be corrupted, the device may break down or malfunctions, and the user themselves can tamper with the data for a benefit [16]. A successful compromise of critical devices such as implanted medical devices used to administer life-saving drugs such as insulin can result in serious or fatal health risks [58]. Before healthcare applications and wireless healthcare can seriously be considered in a large scale applications, these security concerns and health risks associated with health related attacks need to be addressed [58].

2.4.3 INTERNET OF THINGS (IOT)

The prevalence of IoT technology in the healthcare area is growing as patients are more willing to be involved in making decisions about their health [29]. Patients are also more willing to take more proactive approaches to personalizing their healthcare [29]. This personalization of healthcare and treatment can come in the form of smart devices and smart sensors that record and send vital health data to their doctor to remotely view and assess chronic conditions [29]. Examples of these IOT technologies that apply to healthcare and empower patients to make more informed decisions about their health are smart watches, contact lenses, fitness bands, microchips under the skin, and wireless sensors [14]. These wireless systems sometimes do not put as much thought into security as other more sensitive systems such as databases, databanks, and IoT systems have a variety of vulnerabilities and attacks that can compromise security.

Attacks against wireless IoT systems can be categorized as active and passive attacks [59]. A passive attack is categorized as occurring when the data packets are routed through the system and an attacker can change the destination of packets or interfere of the routing protocols [59]. In addition, an attacker can eavesdrop or "sniff" the packets (intercept the packets as they travel through the network or wireless area) to uncover the data contained within [59]. Active attacks are when an attacker uses a vulnerability of a device or network to actively find, steal modify, or obtain information about the user of the device or network [59]. Some of the attacks a malicious actor can use to obtain medical information from IoT devices are: data modification, impersonation attack, eaves dropping, and replaying, which all have the goal of obtaining private information from the victim [59]. Specific security vulnerabilities that attackers can exploit are general system security, administrator security, physical security, and information security [59].

Specific privacy concerns that the healthcare IOT applications experience are identity privacy, location privacy, query privacy, footprint privacy, and owner privacy [62-68]. Third-party cloud providers also have a variety of privacy concerns when it comes to sharing health records among different healthcare institutions [63]. These privacy concerns are access control of patient information and medical data that is used and managed by external service providers [40, 63]. In addition to access control privacy implications, IOT technologies also have

privacy concerns in the form of inference attacks [14]. Inference attacks are when malicious actors use a combination of wireless interception techniques and data mining to infer the value of a given message or signal [14]. Inferred data can then be used to further compromise account through the use of phishing attack to bypass authentication barriers [14]. Wireless networks are also susceptible to active and passive attack from malicious actors in the form of data modification, impersonation, eavesdropping, and replaying of information [58].

There are additional privacy concerns arising from wireless networks and IoT applications. These concerns include: "Can healthcare data be gained from the individual, such as a heart rate monitor, without the consent of the person in an emergency setting" [59]. Privacy related questions that arise from this problem is who should have access to emergency data and how should it be stored [59]. Unless these privacy issues are addressed and patients can be confident in the security of their records in cloud based infrastructures, it is likely that such systems will be widely used [64-68]. These security concerns add to the problem of data sharing and interoperability between medical professionals and institutions [64-68].

In the next section, a brief introduction to blockchain technology and specific features, applications, and limitations as related to the healthcare industry will be introduced.

3. BLOCKCHAIN

Blockchain has been relatively extensively studied since its inception in 2008. For example, there have been studies focused on identifying blockchain applications (e.g. smart contracts and identity verification) [3-5]. In this section, we will briefly introduce blockchain in terms of its features, applications and limitations/issues – see Table 3.

Categories	**Topics**	**References**
Features	Decentralized Storage	[2, 5, 7, 11, 20, 24, 27, 28, 32, 41, 44]
	Security, Assurance, Immutability	[2,4, 5, 7, 8, 12, 14-18, 21, 23, 24-26, 28-30, 38, 44]
	Authentication	[4, 7]
Applications	Smart Contracts	[22]
	Fraud Detection	[39-41]
	Identity Verification	[3]
Limitations/Issues	Lack of Standardization	[3, 7, 22]
	Decentralized Privacy Leak	[26]
	Key Management	[2]
	Scalability IoT Overhead	[5]
	Blockchain Specific Vulnerabilities	[25][40]
	General Software Vulnerabilities	[40]

Table 3 – Blockchain Benefits and Limitations: A Snapshot

3.1 BLOCKCHAIN FEATURES

Blockchain technology has a multitude of features that can be utilized in the healthcare industry. These features are inherent to the system and can be applied to a broad range of systems and industries. The features to be discussed specifically in this section are security, authentication, and decentralized storage.

3.1.1 DECENTRALIZED STORAGE

Decentralized storage is a major feature of the blockchain technology and the basis for the enhanced security and authentication of the information stored within the system [24, 34]. Decentralized storage is the process of breaking up the storage of records from one major server to multiple servers through blockchain's ledger [11], and can facilitate faster access to medical data, system interoperability, patient agency, improved data quality, and quantity for medical research [11, 24]. Blockchain technology can, for example, be utilized by IoT and cloud providers to share data, both securely and privately, in a decentralized manner [24].

Data security, integrity, and immutability are core features of blockchain systems [3, 7, 18, 22]. Blockchain through the use of its confidential secure, decentralized ledger can offer security by storing information among many computers instead of in a single source [3,5,7]. Such a distributed storage method allows a transaction to be distributed through the entire blockchain network creating many redundant data sources to verify the authenticity of the original transaction [3,5,7]. By having this redundancy, a malicious actor cannot make any modification without changing the information on all the systems within the network; thus, allowing for immutability, assurance and security [3,5,7 11].

Data security, integrity, and privacy are growing concerns as they apply to smart devices, public cloud infrastructures, and the general IoT infrastructure [17]. Blockchain can be, in theory, used to secure IoT devices [17, 34]. For example, a blockchain infrastructure allows the cloud services to serve these edge hosts (e.g. smart or IoT devices) as close to the devices as possible with a decentralized nature allowing added security and control [17]. Blockchain also allows secure data sharing by providing data provenance, auditing, and control for cloud based server that store shared medical data among big data entities [19]. This can be accomplished through smart contracts and access control implementations to help securely secure cloud based infrastructures [19]. Blockchain also has applications in technology that allows client request and server reply client-server systems by providing an auditable system to add additional security [21].

3.1.2 AUTHENTICATION

Blockchain through its decentralized infrastructure, also ensures the authentication of records or other private information that is stored in blocks along the blockchain [4]. Authentication is accomplished by requiring a specific private key that is tied to a public key to initiate the creation, alteration, or viewing of information stored in the blockchain [4]. These keys are stored in a variety of software called a Bitcoin wallet and is associated with a Bitcoin address. These software applications are generally applied towards Bitcoin and cryptocurrency, but can be modified for other authentication processes by using the same cryptographic scheme [4]. This authentication is being researched in its ability to authenticate identity and identity documentation ranging from government documents to private healthcare records [4].

3.2 BLOCKCHAIN APPLICATIONS

Blockchain can use its technology and inherent features in a variety of applications across many industries. Applications differ from features as they are not inherent to the system, but instead are processes that the blockchain technology can be applied to, to provide a new requirement. Applications that will be discussed are Smart Contracts, Fraud Detection, and Identity Verification. These three applications were researched for the purposes of the paper due to their ability to solver healthcare related issues discussed in the previous section.

3.2.1 SMART CONTRACTS

Smart contracts are a major implementation of blockchain technology and allow a user or agent to create a legal document through the use of the blockchain system [22]. Smart contracts are an autonomous agent that are stored in a blockchain technology that encode and transform transactions into a contract or legal documents to provide legal services [22]. These smart contracts contain scripts that are stored on the blockchain technology, each with a unique address so that those smart contracts can be traced and verified [22]. Smart contracts provide a means of establishing fair exchange while minimizing interaction among parties in a decentralized manner [22]. A user who has the ability to draft his/her own documents without the aid of a legal representative or notary removes significant challenges, both financial- and time-wise, allowing for more efficient transfer of resources and deeds [22].

3.2.2 FRAUD DETECTION

Fraud detection is another application of blockchain [39]. Fraud detection is the process of verifying a document or other system of data to identify any tampering with the information or other malicious conduct [39], such as preventing the injection of false reviews in online review systems in the form of bad-mouthing and ballot-stuffing, as well as fact-based fraud in financial sector such as loan applications [39, 40].

Another area of fraud detection study is directed at the relatively recent concept of crowdfunding [41]. Crowdfunding is the process of having large number of people either investing money or buying stock from a company to raise equity for that company [41]. Blockchain can be used in a crowdfunding function by, making transactions and transfering of crowdfunding equities easier, more secure, and efficient, as well as being leveraged as a low-cost platform for registering of stocks and shares, enabling peer-to-peer transactions between investors and

entrepreneurs. Blockchain can also be used to develop a voting system for corporate governance among shareholders, and help regulators know about market conditions and protects against investor fraud [41].

3.2.3 – IDENTITY VERIFICATION

Beyond the healthcare industry, many online businesses have found varying methods of verifying identity. Currently, many businesses and government use passports and fingerprints to identify individual [4]. All documents are prepared and validated by the government, but blockchain is providing an alternative to government sponsored identity verification [4]. Blockchain has the ability to verify the identity of the user outside of these government [4]. An example of this application is to use blockchain to notarize marriages, birth certificates, and business contracts [4]. The blockchain would use the distributed ledger to allow a person to prove he/she exists at a certain time and place, and is verified by a group of individuals through the use of the distributed nature of blockchain.

3.3 BLOCKCHAIN LIMITATIONS / ISSUES

Despite all the advanced features Blockchain provides , it still has a variety of limitations and issues that need to be addressed. The specific limitations to be discussed in this study are a lack of standardization, privacy leakage, key management, IoT overhead, and blockchain specific and supporting software vulnerabilities.

3.3.1 LACK OF STANDARDIZATION

As a relatively new and immature technology, there is a lack of standardization and this hampers its broad acceptance and slows down development [3]. Many countries are considering the adoption of blockchain technology in government settings, such as voting [3, 42]. Countries, such as Estonia, are looking to merge their residency requirements with blockchain technology to create e-residency, which is the process of creating an online account to verify a citizen's residency in that state and enables them to vote through this online capabilitiy [4]. Other researchers have also examined the possible use of blockchain technologies in their tax and social frameworks [43]. To enable all of these differing infrastructuers and applications, there needs to be a high level of standardization across the various parties involved. As more countries begin to adopt blockchain as a solution, this issue of standardardization and requirements will continue to increase in importance [3].

3.3.2 DECENTRALIZED STORAGE AND PRIVACY LEAKAGE

Decentralized storage is one of the key unique features of blockchain systems as it allows users to share data among different services without a centralized service provider [26]. However, the key disadvantage of decentralized systems is the potential privacy leakage, since a user has to retrieve data from the public ledger that is distributed among the blockchain system. When a user retrieves his/her data, the user needs to enter a private key to verify and decrypt the information from cypher text to plain text resulting in a potential privacy leakage. As the information is not stored locally, such as in the case of a centralized database, the public key has to be within the network when the process of verifying and decrypting is initiated. This is problematic in healthcare settings, due to the exacting requirements of the sector.

3.3.3 KEY MANAGEMENT

Data stored on the blockchain ledger needs to be secured through a variety of cryptographic processes that require the use of private and public keys [2]. Blockchain technology, like any other form of technology that has the potential to store information, needs processes in place to ensure security and privacy. Most cryptographic processes require keys to enable those cryptographic processes because blockchain data is stored publicly and is shared by all participants; thus, requiring some level of encryption / access control [2]. Current key management principles are not feasible for blockchain as one key for all blocks is unsafe because if the key is compromised, then all data will be leaked. However, one key per block is not practical as it requires a high cost to store and recover the (significantly) large number of keys for each individual block that has ever been created.

The role of blockchain in cloud data infrastructure is facilitating the creation of a decentralized and trusted cloud data provenance architecture that allows tamper-proof records, greater transparency of data accountability, and enhanced privacy and availability of the data [26]. Another application of blockchain technology is a secure data bank that allows users to store personal healthcare records and information allowing more interoperability and sharing of data among healthcare providers [27].

3.3.4 SCALABILITY AND IoT OVERHEAD

Another limitation of the blockchain system is in the form of scalability and the increased overhead or computational resources in an IoT environment. Scalability in blockchain systems is a concern as the number of

participants in the system also increases the computational requirements of the entire blockchain infrastructure [10]. This becomes an increasing challenging issue if there are a large number of smart devices or sensors as the computational ability of those devices is less than an average computer, offloading much of the resource requirements to other computers, such as an edge device or the cloud [42].

In an IoT setting, a number of IoT blockchain specific solutions are computationally expensive and involve high bandwith overhead that results in delays of data and significant processing power [44]. Such requirements are impractical for most IoT devices since they are generally sensors and are computationally constrained. In other words, such devices may not have the required computational power to utilize blockchain capabilities, while fulfilling their original purpose [42]. This slow-down in processing speed can result in the devices performing sub-optimally or potentially even over taxing the device making it unable to even run the original software or blockchain program at the same time [43].

3.3.5 BLOCKCHAIN SPECIFIC VULNERABILITIES

Blockchain technology also has a few specific vulnerabilities that are unique to the system's implementation and architecture. Blockchain specific vulnerabilities include block withholding attacks, 51% attacks, double spending attacks, selfish mining attacks, eclipse attacks, block discarding attack, difficulty raising attack, and anonymity issues in blockchain [25, 40]. A core mechanism of blockchain is the consensus mechanism that allows blockchain to build a tamper-proof environment, as transactions on any digital assets are verified by miners or a set of legitimate participants that authenticate each transaction [25]. Miners need to expend significant computational power to authenticate transactions and usually need an incentive to complete the authentication, which is often the solving of a cryptographic equation [25].

A withholding attack is one when malicious actors successfully mine blocks, but do not submit those blocks back into the system. Instead the miner only submits shares of the block that are not the complete solutions required by the system. These shares are only a portion of the solution and do not result in the block being mined and decrease the expected revenue of the pool as each share reduces the ability for another miner to submit a successful solution [25]. The result is that a malicious actor by withholding the complete valid blocks limits the ability for others submit a full solution, and thus reducing their revenue. However, such an act increases the rewards of the malicious actor since the latter can submit as many shared blocks as possible to the authenticating pool manager, which each have a portion of the solution [25]. A similar attack to withholding attack is a 51% attack, where a single miner has more computational resources than the rest of the network and dominates the verification and approval of transactions on the blockchain controlling the content of the blockchain [40].

A double spending attack is the process of using the same digital cryptocurrency for more than one transaction by easily reproducing the digital information for the cryptocurrency [25]. In a selfish mining attack, selfish miners intentionally invalidate the work of honest miners by strategically publishing the private chain mining pool at specific states of the pool to influence the rewards [25]. An eclipse attack is an attack that takes advantage of the peer-to-peer network that the blockchain uses [25]. Specifically, the eclipse attack takes advantage of the randomly selected eight peers to maintain the connection and storage of the peer network by rapidly repeating unsolicited connection requests to greatly increase the change they are the eight nodes to maintain the connection for malicious purposes [25].

A block discarding attack is the process of getting a good hold of network connections compared to other nodes and using this connection to get informed of mined blocks before the rest of the network. Then, the attacker publishes the mined block before the legitimate miner and discards their blocks [25]. A difficult spike attack is when an attacker takes advantage of the hashing power of the cryptographic process of mining blocks to manipulate the difficulty level [25].

Another potential blockchain vulnerability is its pseudo-anonymity, which is the fact that all transactions are permanently recorded in the public ledger and anyone can see the transaction. The private information is kept private until the information is revealed in some circumstances, which would allow anyone to use that information to look up past transactions from that user [25]. Such information can, however, be useful in an audit trail or a forensic investigation. There is another form of Blockchain specific attack in the form of a forkable attack. A forkable attack is based on the concept that when participants in a blockchain structure must agree on the possible branches that the blocks of the blockchain will form after being mined and validated [45]. Due to this process, a theoretical attack (known as a balance attack) can be performed where a malicious actor can mine a branch potentially in isolation of the rest of the network before that actor, and merging that branch to one of the competing blockchains to influence the branch selection process [45, 46]. This is accomplished by leveraging the GHOST protocol that accounts for a block, called a sibling block or uncle block, that selects the chain of blocks [45, 46]. A last consideration for blockchain is to properly incentize miners. If the miners do not receive any benefit for the

computational resources they pour into facilitating the blockchain, then they may not facilitate transactions or the creation of new blocks [11].

3.3.6 General Software Vulnerabilities

Blockchain is also vulnerable to some general software vulnerabilities that allow for malicious attacks. These malicious attacks can then be used to facilitate other offenses such as identity theft and data exfilitration [40]. Identity theft occurs on blockchain if a user of blockchain has his/her private key stolen, which allows the malicious actor to have access to everything the victim ever published on the blockchain [40]. Illegal activities such as illegal guns, drugs, and other contraband can be sold through the distributed ledger in a pseudo anonymous fashion. In addition, poorly maintained blockchain implementation software like a bitcoin exchange can be hacked allowing the implementation of double-spending of bitcoins or other cryptocurrency [40, 47].

The next section will discuss existing literature focusing on blockchain related healthcare applications.

4. Existing Blockchain Literature for Healthcare

Blockchain has numerous potentials for healthcare technology. There are a variety of existing experiments and literature highlighting blockchain enabled healthcare applications and a few specific software solutions will be discussed in each section below.

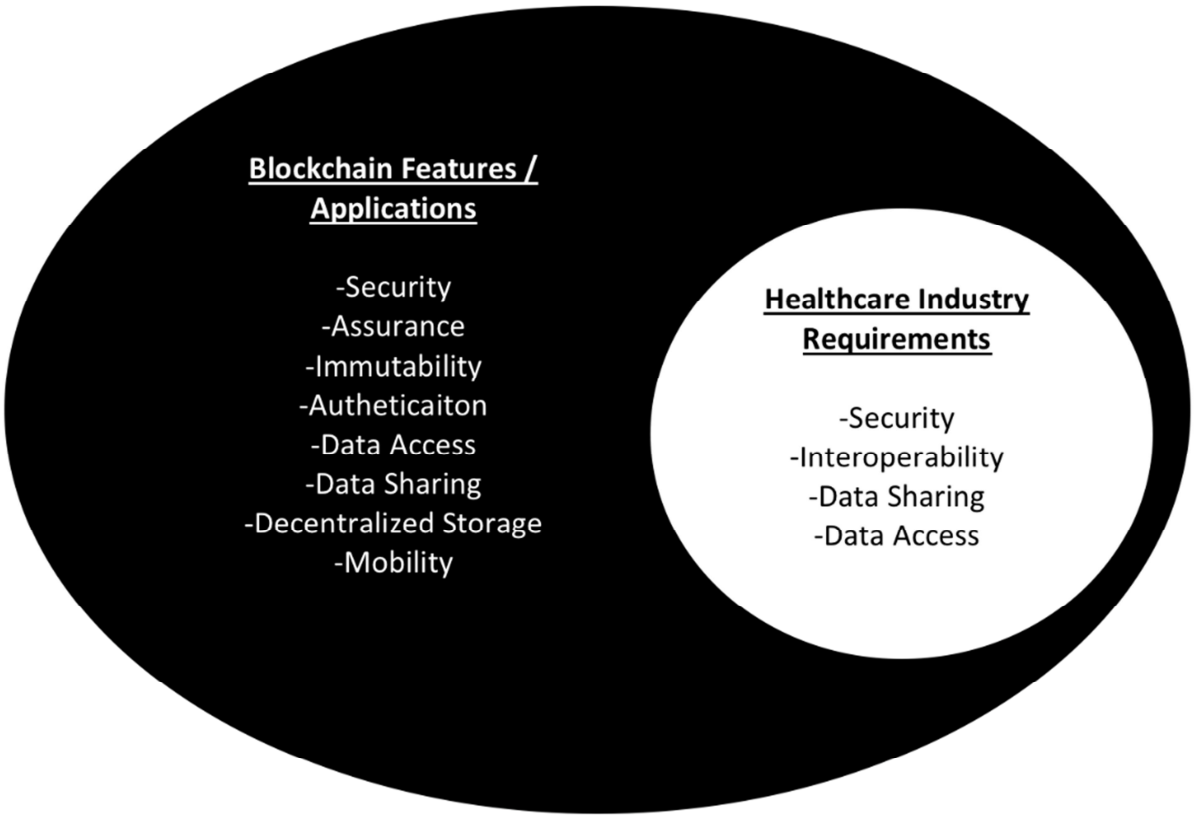

Figure 2 –How Blockchain meets Healthcare Requirements

4.1 Healthcare Datasharing through the Gem Health Network

The healthcare industry handles many records and documents that are confidential and fall under strict laws such as Health Insurance Portability and Accountability Act of 1996 (HIPAA). Such records are generally stored in a centralized database, which may result in issues such as security and interoperability discussed in the preceding section [37-39]. The difficulty of sharing confidential records is a problem can occur when a patient is in need of specialized treatment at a different hospital, interstate or overseas (e.g. when a 'medical tourism' operation goes wrong in an overseas hospital and the patient requires urgent medical treatment). Each time the patient sees a

different professional, there is a disruption due to the need of creating new records, changing communication protocols between doctors, updating of various medical health records, and incompatible IT interfaces that can lead to time-consuming and resource-intensive authentication and information processing for all parties involved [12].

A potential solution to this problem has been developed by *Gem Health Network* [12] that used the *Ethereum Blockchain Technology* [12] to create a shared network infrastructure. *The Gem Health* Network allows healthcare professionals to all access the same healthcare information removing the limitations of centralized storage. The medical records and information are relevant, transparent, and authorized users have real-time access to the latest treatment information [12]. This can help minimize the risk of medical negligence due to outdated information and prevent health issues that may arise from that misinformation [12].

Estonia has reportedly collaborated with *Guardtime*, which is a healthcare platform that uses blockchain technology. This allows Estonian citizens, healthcare providers, and health insurance companies to retrieve all medical treatments performed in Estonia by using the technology. This suggested the utility of blockchain to be utilized in the manner discussed above [12].

The *Gem Health Network* attempts to address the issue of sharing patient records in a seamless environment between both patients and physicians. There are, however, a number of challenges that need to be resolved, such as identity management for the patient and if there is any type of key management to secure the records from tampering and abuse. Additionally if a public key is lost or leaked, how can the information be recovered and the compromised key be updated?.

4.2 OMNIPHR

OmniPHR is a model developed by Roehrs, Costa, and Righi [10] to help handle patient health records; thus, giving patients a unified view of their health records stored across multiple healthcare providers [10]. In addition, the OmniPHR framework is designed to address the problem of healthcare providers having access to up-to-date data regarding their patients, even when the records are stored in another location or have been updated by other healthcare providers [10]. The main issue that OmniPHR seeks to address is the difference between electronic health records (EHR) and PHR. EHR are records that are held to a variety of governmental standards that help to address the problem of uniform record keeping across state and country lines [10]. This allows the records to stay up-to-date and as accurate as possible [10]. The main consideration for these records is that they are held and updated by the medical professionals themselves without any patient interaction, which differs from PHR, which are handled by the patients themselves [10]. OmniPHR helps to create a framework that would address this problem allowing patients to have a more comprehensive and complete picture of their records, while maintaining the level of accuracy desired by the medical community [10].

Specifically, OmniPHR is a functional model that incorporates blockchain technology that focuses on the distribution and interoperability of PHR data with the goal of allowing a unified view of health records that are distributed across several health organizations [10]. In addition, OmniPHR attempts to address the challenges of having a distributed architecture that is scalable, elastic, and interoperable. The PHR would be stored and organized hierarchically and be encrypted as well as distributed in chained datablocks on the network. The model is setup to differentiate the users that join, either as providers or consumers. The patients can be at home, at work, or at a hospital to fulfill the goal of having the model be everywhere. Providers can differentiate the devices that can supply the data to compose the PHR, as well as the users can use devices that can read the PHR data.

The model is set up as a P2P (peer to peer) network with a routing overlay through the use of an application server with defined responsibilities. It also has cloud-related features that include elasticity and horizontal scalability [10]. There are a few components that make up the model, which are data sources, a proprietary open standard, middleware, encryption protocol, privacy module, and respositories [10]. Data sources flow through the model by first being fed into a proprietary or an open standard and then converted through the middleware [10]. Next, the data sources are encrypted and authenticated in a security and privacy module, prior to being stored in a series of repositories [10]. OmniPHR uses laboratory data to evaluate the performance of the model. OmniPHR also uses an open standard, openEHR, that promotes interoperability by organizing datablocks hierarchically [10].

OmniPHR was evaluated in an university setting with a simulated dataset [10]. The main findings were that with the network architecture was able to handle an increasing number of users and requests without increasing the delivery time significantly, and that the Chord algorithm was able to segment the datablocks in clusters that allows the network to decrease the number of hops it took to access the records [10]. This results in a stable or decreasing latency.

A key limitation is that the data had to follow the standards supported by the model and if the data was not within the scope of the standards it would not be shared [10]. The patients and healthcare providers are responsible for verifying and entering varying data such as demographics for the patient and the diagnosis for the healthcare

provider [10]. Another limitation is the fact that the patient has to authorize access for anyone else to access the record as by default only the patient and a healthcare provider have access to the data [10]. Key management and key recovery is also a problem not considered by OmniPHR in the case of a lost or leaked key.

4.3 MEDREC

Medrec developed by Azaria, Ekblaw, Vieira, and Lippman [11], is a decentralized record management system to handle EMRs using blockchain technology. The system allows patients real-time access to their medical information across multiple medical providers and treatment locations [11]. Specifically, blockchain technology is used to facilitate authentication, confidentiality, accountability, and data sharing through the use of a modular design that integrates with providers' existing, local data storage [11]. This solution allows the patients and medical professionals to have interoperability [11]. As previously discussed, blockchain requires a series of miners to help facilitate the blockchain transactions process. MedRec incentivizes medical stakeholders to participate as the miners by providing them access to aggregate, anonymized data as mining rewards in return for sustaining and securing the network via PoW [11]. Such incentives (data economics) allow patients and providers the choice to release their data as metadata [11]. MedRec is a working prototype that focuses more on analyzing the approach and implementation of the framework, prior to any field tests.

MedRec is composed of block content that represents data ownership and viewership permissions shared by members of a private P2P network [11]. MedRec is also made up of smart contracts that allow the model to automate and track state transitions, such as the change in viewership rights, or the addition of a new record [11]. Smart contracts are implemented through the Ethereum blockchain and log patient-provider relationships that associate a medical record with viewing persmission and data retrieval instructions [11]. The information is encrypted and patients can authorize the sharing of records between providers with any change or new information being added [11]. The change of information is accompanied with an automated notification that allows the patient to verify the proposed record before accepting or rejecting the data [11]. All patient-provider relationships are aggregated and referenced in a designated contract resulting in a single point of reference to check for updates in the medical record [11]. Identity confirmation is handled via public key cryptography and employs a DNS-like implementation that is applied to an existing and widely accepted form of ID such as a social security number [11].

The MedRec model is comprised of a registrar contract, summary contract, and patient provider relationship contract that helps to identify the patient, hold the patients information, and compile any relationships the patient may have [11]. In addition, there are provider nodes and patient nodes which are authenticated and created through the use of the Ethereum Blockchain technology and facilitated by miners [11]. Overall the model is a representation of the benefits of a decentralized database structure that allows patients and providers to share information among each other without a single point of failure improving interoperability of record sharing. Another benefit of the system is the fact that it addresses the problem of data mining incentives, which is a pressing problem when it comes to medical oriented blockchain implementation [11]. The system does attempt to solve identity management using the system's DNS-like implementation.

The main limitations of the infrastructure are that is does not address security of an individual databases, attempt to solve digital rights management problems, and the pseudoanonymous nature of the blockchain infrastructure allows the use of data forensics to infer the patients and providers relationship [11]. Blockchain technology also struggles to scale the technology for high transaction volume [11]. The proposed system does not attempt to address the issue of having a patient who is in an emergency situation (such as an unexpected access) giving permission to access their records to a surgeon not previously authorized. The system assumes the patient has the foresight to enable permission, which may be unrealistic in a real-world setting. This necessitates the design of a customized / two-tier access control system that allows a trusted user (e.g. a medical practitioner in another hospital that has been vetted appropriately, for example by the country's Department of Health) to gain temporary access to another user's data when certain conditions are met (e.g. a medical or a life-threatening emergency).

4. 4 PERVASIVE SOCIAL NETWORK (PSN) SYSTEM

A prosed secure system for pervasive social network (PSN) was proposed by Zhang, Zue, and Huang [13]. A PSN is a network based healthcare system comprising mobile computing and wireless sensing [13]. The core problem that stops a PSN from being a fully realized concept is how a PSN node can securely share health data with other nodes in the network [13]. The researchers attempted to solve this problem by proposing two protocols to secure a PSN based healthcare system [13]. The first protocol is an improved version of the IEEE 802.15.6 protocol that handles the display of authenticated association by establishing secure links with unbalanced computational requirements for mobile devices and resource-limited sensor nodes. The protocol establishes these secure links for sensor nodes and mobile devices in the WBAN area. The second protocol uses a blockchain technique to share

health data among PSN nodes by using the addresses in the blockchain to facilitate a way for other PSN nodes to visit each other in the network and access health data.

The PSN system is proposed through the use of these two protocols to help establish a blockchain enabled healthcare data system that can share data among smart devices and sensors between a patient and their physician. A use case or demo system for this implementation is Alice, a patient with hypertension, consults Bob, an expert on the disease. Also, Bob wishes to gain the information that is stored on Alice's wearable blood pressure monitor [13]. To gain access to this information using the PSN blockchain system, the following steps must be taken: Alice needs to establish a secure link between the wearable wrist band and her smartphone. The smartphone then broadcasts a blockchain transaction to the neighbor PSN nodes, which is received by a miner node. The miner node creates a new blockchain generation generating a signature in the process to verify the new block, and the last step is for Bob to access the data using his smartphone [13]. The system acts more of a facilitator of sharing information between hospital networks, rather than being a complete solution for healthcare interoperability and security.

The advantages of this system include the following: (1) the network reduces the computational burden on the blood pressure monitor (an IoT device), (2) it avoids incurring significant storage requirements at the PSN nodes, and (3) it also avoids potential data leakage due to an untrustworthy third party since the data is stored on Alice's device locally [13]. However, the system does not address the key management issue of blockchain resulting from a lost key or a leaked key.

4.5 Virtual Resources

Virtual resources, a concept proposed by Samaniego and Deters [15], use restful micro-services, and are designed to be used as a software-defined IoT management construct. The latter is designed to facilitate multi-tenancy support and shift load distribution to some edge hosts (systems that are more computationally capable than IoT devices). The proposed system seeks to solve the following problems associated with IoT edge devices: (1) the lack of support for virtualization and abstraction, particularly on constrained and heterogeneous edge components, (2) the lack of a mechanism to facilitate secure software distribution for edge hosts, and (3) the lack of an efficient access control management for edge-hosted software [15]. Virtual resources enable the ability to create a virtual IoT system on top of an existing IoT system. Since it is a restful service, it allows one to view one or more IoT components. It is also a digital artifact that is linked to any other IoT component including other virtual resources [15]. Virtual resources process requests by engaging other restful services or by using their internal state and by defining these views on top of existing components, and it is possible to create any number of virtual IoT systems on top of an existing IoT system [15].

This process allows virtual resources to become a mechanism for: handling multi-tenancy since each tenant uses their set of virtual resources, distributing loads since these micro-services can be hosted closer to the edge, and enabling controlled low-latency access to things as well as a mechanism for distributing loads [15]. To enable the secure deployment of code, a main challenge of edge devices is to enable permission-based blockchain support [15]. Blockchain would have code or a signature be pushed into its infrastructure and the edge devices would then pull the information from the blockchain, and as demonstrated by IBM's ADEPT system it is possible to push code into IoT devices without having any safety or security issues raised by the devices [15]. The researchers were able to use a blockchain based infrastructure in the cloud-hosted IBM Bluemix to create a permission-based blockchain approach to virtual resources [15]. The purpose was to add security to the virtual resource deployment, and their experiment showed a fluctuation in latency between 0 and 300 milliseconds. This can be explained due to the fact that the blockchain service is free and therefore, more likely to experience significantly fluctuating loads. Consequently, this results in greater variation in its response time. However, findings of the experiment performed by the authors suggested that the permission-based blockchains could potentially be used to store virtual resource state data [15].

4.6 Context-driven Data Logging for Bodyworn Sensing Devices

Context-driven data logging, developed by Siddiqi, Ali, and Sivaraman [16], is a lightweight scheme designed to securely log the data from bodyworn sensing devices (also referred to as wearable devices in some literature) by utilizing neighboring devices as witnesses who store the fingerprints of data in Bloom filters to be later used for forensics. The concept arises due to the challenge in recovering forensically sound evidence from wearable technology. As these devices and the data they collected are increasingly used by firms such as John Hancock Insurance, United HealthCare Group, and MLC as well as other medical industries, it is important to also understand the risks involved as well as challenges when it comes to the data being sent from these devices [16]. Risks include corruption of data, fault in devices, or the tampering of data by a malicious third party (e.g. to claim benefits). For example, it had been demonstrated that it is possible to exploit medical sensing devices to allow a third-party to

backfill medical data [16]. It has also been reported that the former US Vice President Dick Cheney was concerned that he could be assassinated via his embedded wireless pacemaker [69].

The proposed framework to create a system with secure logging and data provenance is through the use of chaining together blocks of readings from successive epochs to prevent retroactive tampering with data (this concept loosely borrows from the blockchain technology), as well as incorporating Bloom filters on sensor devices to ensure that the scheme is lightweight and not resource intensive [16]. A Bloom filter is a space-efficient probabilistic data structure that is a compact way to store data where the requirement is to enquire membership and not to retrieve the data itself [16].

The specific architecture consists of a gateway that maintains a detailed log of all conversations that it conducts with sensor devices, which the gateway then converts and forwards in epoch-level blocks to a centralized server [16]. These blocks loosely follow the same structure as blockchain technology by being grouped together or chained, so that each successive block contains a hash value of the previous block and the chain is replicated in multiple locations to prevent retroactive data tampering [16]. In addition, sensor devices log all communications they overhear on the network between any other parties in that same network and maintain a record, which is later forwarded to the gateway acting as witnesses for the record [16]. To filter out the potential problem of large memory or communication overhead in the situation there are many sensor devices communications, Bloom filters were used to log (or fingerprint) all transmissions they hear as Bloom filters considerably reduce the memory consumptions and transmission of the communications over the network as well as adding simple and accurate verification [16]. To ensure the gateways and the sensors can communication a synchronization protocol is used at the start of each epoch and at the conclusion of each epoch, all witnesses upload their Bloom filters to the centralized server and all fingerprint data are digitally signed by the witnesses, which can be later used to verify or certify the data through the use of data forensics [16].

An experiment was performed that used a sensing device that transmitted a data at a rate of 1 packet/sec. A range of witnesses (i.e. 1-10) were used at random to log the data at varying probabilities, depending on the number of witnesses veryfing the packet [16]. The experiment found that with the ideal configuration, the scheme was able to give an accuracy of 98.5% in verifying a packet, a trust of 90% with 47% savings in the cost versus the second configuration in the experiment [16]. For the purposes of the experiment, trust was defined by a parameter referred to as the Trust Defining Parmater. The latter defines the value of trust based on the number of witnesses for that packet [16]. The experiment showed that blockchain technology could be used to inspire other frameworks to help add a level of confidence and validity to data being sent through IoT or body worn devices. A consideration for the project was that there was no inherent security such as encryption, but had the ability to be added on in the future [16].

4.7 MEDSHARE

MeDShare , developed by Xia, Sifah, Asamoah, Gao, Du, and Guizani, is a system designed to address the issue of medical data sharing among medical professionals that store data in a trust-less environment [19]. A major problem in the health industry is to maintain privacy for patient records, and reduce the risks of malicious activities on medical records that can cause severe damage to reputation and financial loss for all parties involved [19]. The system is built upon blockchain technology and provides data provenance, auditing, and control for shared medical data in cloud based environments among large companies [19]. MeDShare monitors entities that access the medical data and checks for malicious use from any party that tries to access that data [19]. All data transactions in the MeDShare system are shared from one entity to another entity, with all actions performed recorded in a secure manner to prevent tamper-proof [19]. The design uses smart contracts and access control mechanisms to track the data and revoke access to any malicious entity on detection of any violation or misbehavior within the system [19]. The main goal of MeDShare is to give cloud service providers and other entities storing sensitive medical data the ability to achieve data provenance and auditing, while sharing medical data with entities in the medical community with little to no risk to the data privacy of the shared records for the patients involved [19].

The MeDShare system is built using blockchain technology and is split between a series of four main layers [19]. The first layer is a user layer that consists of all the different classifications of users who want to access the data from within the system. The second layer is the Data Query layer that consists of sets of querying structures that access, process, forward, or respond to queries posed on the system. These processes are then split between two main components, namely: the querying system that is responsible for processing the request, and the trigger that is responsible for translating actions to and from the smart-contract environment. The third layer is the Data Structuring and Provenance layer that consists of individual components that help process request for access to data from the existing database infrastructure through a series of entities, These entities are in the form of an authenticator, processing and consensus nodes, smart contracts, smart contract permissioned database, and the

blockchain network. The last layer is the Existing Database Infrastructure layer that consists of already established database systems implemented by individual parties to accomplish specific tasks. MeDShare [19] demonstrated that it added a level of security to cloud based interactions through its security, but the main limitation of the system was as the number of requests on the cloud-based service increased so did the latency. MeDShare was able to create a level of confidence and data provenance, but the downside of a significant addition of latency and time to add or retrieve data if there were many other requests being sent to the system [19]. Key management and recovery were also not addressed, similar to the other systems discussed in this paper.

4.8 Blockchain Platform for Clinical Trials and Precision Medicine

Blockchain platform for Clinical Trials and Precision Medicine (Trial and Precision Medicine) is a blockchain platform architecture proposed by Shae, and Tsai [18], for clinical trial and precision medicine [18]. The benefits of the proposed system first start with an added data integrity in clinical trial data, which addresses the problem of clinical trial researchers incorrectly reporting their data. In other words, the blockchain paradigm allows more transparency and help improve the accuracy of the data analytics performed on the data gathered from the clinical trials [18]. Another benefit would be that the blockchain would enable peer verifiable clinical trials. This allows peers to evaluate and test the data from the clinical trials, without the data owners (e.g. clinical trial researchers) losing ownership of their data [18]. This system architecture seeks to fix two problems with the clinical trial data process, and that is peer verifiable data integrity and data sharing and trust collaboration [18]. The proposed system solves these issues by having verifiable anonymous identity privacy and secure data access through the use of the blockchain architecture [18]. The system hopes to use a decentralized platform making legal and regulatory decisions about collection, storing, and sharing patient data simpler, as well as letting patients have control of their own data rather than a third party, and the patients are always aware of who access their data [28].

The blockchain architecture is built up of four system components that are required on top of the traditional blockchain construct [18]. The traditional blockchain platform (that is used for the Trial and Precision Medicine architecture) is made up of a distributed ledger, messaging protocol, smart contract, proof of work or stake consensus algorithm [18]. On top of the blockchain architecture, the researchers proposed four additional components in the form of: data sharing management, application verifiable anonymous identity management, blockchain data storage management, and a new blockchain based distributed and parallel computing paradigm [18].

This new modified blockchain architecture would then be deployed between inputs and outputs. The inputs would be published medical papers, medical question knowledge database, stroke database, analytics method knowledge database, and a database (and in the context of the paper, a Taiwan national health insurance database). The outputs would be sematic similarity model, structure natural language GUI, keywords analytics, questions and analytics method extraction and medical data. The blockchain architecture would be between the inputs and outputs to add a level of integrity and security to the medical data.

4.9 Healthcare Data Gateway

The blockchain-based Healthcare Data Gateway (HGD) proposed by Yue, Wang, Jin, Li, and Jiang [28], is designed to facilitate patients taking control of their medical records. In other words, patients can more easily own, control, and share their data securely. The HDG was developed to support smartphone application and was chosen due to its mature computing power, the popularity of Smartphone application stores, its popularity, and the fast mobile wireless network that support cloud-based 5G network. The application would enable a gateway that consists of three layers, namely: a storage layer that provides scalable secure, highly available, and independent storage service for health data, a data management layer that consists of a set of individual's HDGs that are independent and connected with each other, and a data usage layer that allows entities that use patient healthcare data to access the medical record systems [28].

In an example scenario, John is a patient and Roger is his physician and John can decide to share his blood test data by decrypting the blood test data and encrypting it with a new key and sends the data with the new key to Roger [28]. Roger then uses the key that John sent to query the data, but while Roger's HDGs holds John's data replica, Roger cannot operate on the replica exceeding their authorities and the HDGs will enforce to destroy the replica after one data period or after the authorized period has expired. All of Bob's actions are recorded by John's HDGs and sent back to John for audit purposes [28]. If Roger issues a new blood test, then the test results are sent to John's account in the blockchain cloud in an encrypted form and fed to John's HDG. If the data is to be kept secret, then the file can be masked and hidden from users querying the healthcare data except for him [28]. The infrastructure also allows someone to query how many people have the same condition as John, so a counting function is called and each HDG generates one random value and keeps it securely [28] Next, the HDG adds the random value and 1 to the counting value if the patient has the same disease. After the HDG finishes counting, it

subtracts the sum of all the random values from the results [28]. The results of this process will report the number of people who have the same condition without reporting what which patients have the specific condition [28].

In addition, the HDG uses a unified data schema to help store and organize data in a database management system, a data query system that is based on access purpose, data management functions that emphasize privacy protection, anonymization, communication for data requests or collaboration, and data backup and recovery [28]. The system uses the decentralized platform to facilitate legal and regulatory decision-making relating to collection, storing, and sharing of patient data, as well as allowing patients to have control of their own data. In addition, the patients are always aware of who access their data [28]. Even though HDG attempts to facilitate secure data sharing while maintain privacy, it does not address the issue of granting termporary access to user data during emergency situations (see Section 4.3). There is also no capability to replace a lost or compromised key.

In the next section, we will present the discussion.

5. DISCUSSION

As summarized in Table 4, blockchain has been studied and applied to the healthcare industry with specific blockchain software solutions. These practical solutions have been evaluated or deployed in a University laboratory department set to mimic a real-world setting.

Types of Evaluations	**Dataset Configuration**	**Type of Information**
Laboratory	Closed-source: Virtual network of nodes, routing overlays, and backbone routers [10]	Simulated messages that denote patient records
	Closed-source: Virtual network of PSN nodes connected to a Laptop and Rasberry Pi [13]	Simulated messages that denote patient information
	Closed-source: Virtual network of two Intel Edison Arduino boards with hosted Virtual Resources [15]	Sequential requests
	Closed-source: Virtual network consisting of three MicaZ sensor devices [16]	Medical information obtained from a worn sensor device
	Closed-source: Virtual network consisting of a range of users to determine latency in the blockchain infrastructure [19]	Simulated messages that denote patient information
Real-world	None	

Table 4 – Evaluations

These technologies were conducted in a laboratory setting with a closed-source dataset. The specific research papers with evaluations that were reviewed in this literature review were: OmniPHR, PTSN, Virtual Resources, Context-driven Data Logging, and MeDShare. The OmniPHR model used a dataset that was generated in a laboratory environment with a closed-source dataset using the Oversim framework to represents overlay and P2P networks, which is an implementation of the discrete event network environment OMNeT++ and the INET Framework, which is an open-source suite of models for wired, wireless, and mobile networks to OMNeT++ [10]. The data was generated by having a variety of environment settings including ten network setups with two different tests for each one being executed [10]. The setups conducted involved 100 nodes with differing amounts of routing overlays and backbone routers increasing from 4 to 80 routing overlays and 1 to 40 backbone routers [10].

The PSN was evaluated by conducted a series of experiments in a laboratory setting with a closed-source dataset. There were three main experiments conducted using a protocol suite and a sensor that is deployed on a Raspberry Pi with a coordinator on a laptop [13]. The experiments purpose is to evaluate the overall burden of the protocols from two aspects: communication cost and computation cost to demonstrate the effect of a real-time deployment of the protocol suite [13].

Virtual Resources was evaluated in a laboratory setting with a closed-source dataset using two Intel Edison Arduino board [15]. Both boards used in the experiments were both connected to the same shared WiFi network

[15]. The first experiment was conducted with each board running one virtual resource and one virtual resource sent 1000 sequential requests to the other virtual resource with the virtual resource waiting for an acknowledgement after sending the request before sending another request [15]. The second experiment each board hosts ten virtual resources concurrently and each virtual resource sends 100 requests to the virtual resource hosted on the other board [21]. The third experiment had a single board used with ten virtual resources running concurrently issuing 100 sequential write requests to the cloud-hosted blockchain which was implemented by IBM Bluemix [15].

Context-driven Data Logging conducted experiments in a laboratory setting with a closed source data-set. The experiment was conducted with real wireless devices and a human subject wearing a MicaZ mote on the arm [16]. The sensing device was worn for half an hour as the subject walked around and the MicaZ mote acts as a gateway while three other motes act as witnesses (two were stationary and the third was mobile) [16]. The sensor transmitting at the rate of 1 pkt/sec at maximum transmission power, while the other sensors were set to log any communications they heard [16].

MeDShare conducted experiments in a laboratory setting by simulating real-case scenarios where cloud service providers shared data among other cloud providers in a closed-source dataset [19]. The experiment was conducted by establishing the MeDShare infrastructure, with an algorithm to handle smart contracts and then simulated interactions on a cloud service provider, access policies stored as records in blocks, and the permissions database assigns different permissions to users for available services were all conducted and evaluated [19]. Analysis was conducted on request of data, data retrieval, and processing, which includes the generating of smart contracts and tagging of smart contracts on package, and monitoring of actions on data using JMeter [19]. The experiment also looked to see if there were any inconsistencies and violations to demonstrate vulnerabilities within the system and latency was also evaluated and measured [19].

Application	**Benefits for the Healthcare Industry**	**Blockchain Specific Challenges Addressed**	**Limitations**	**Focus of Work**
Gem Network [12]	Sharing of Health Data through Decentralized Network and legal issues addressed	N/A	Scalability is not addressed, key replacement capability is not provided	Third-Word Countries such as Estonia
OmniPHR [10]	Sharing of Patient Records	Scalability	Data has to fit OmniPHR standard or is rejected, user has to authorize all access requests, and potential duplication of data	Laboratory
MedRec [11]	Sharing of Health Data	Mining Incentives	Security, no key replacement capability, and legal issues are not addressed	Laboratory
PSN [13]	Sharing of Health data on IoT Devices	N/A	Scalability is not addressed, key management and leakage is not addressed	Laboratory
Virtual Resources [15]	Storage of Health Data in a framework that stores persistent data storage that is safe, secure, and scalable	Potential standardization challenge addressed through proposed framework	Scalability is not addressed, no key replacement capability	Laboratory
Context-driven Data Logging [16]	Storage of Health Data and adds a level of confidence to data logging	N/A	Security is not addressed, no key replacement capability	Laboratory
MedShare [19]	Authentication, Security and sharing of medical information	N/A	Scalability and latency problems, no key replacement capability	Laboratory

Trial and Precision Medicine [18]	Integrity and data access security	N/A		Clinical Trial Databases
Healthcare Data Gateways [28]	Security, authentication, and legal issues with data sharing	N/A	Scalability is not addressed, no key replacement capability	Laboratory

Table 5 Blockchain Research – Challenges and Benefits

The discussed blockchain articles have numerous features and applications that can be deployed in the healthcare industry, as well as limitations – see Table 5. The major benefits explored in many of these experiments come in the form of having a decentralized structure, allowing interoperability, security, authentication, and integrity. Major problems associated with a deployable blockchain framework are the scalability, mining incentives, blockchain specific attacks, and key management / key leakage.

Each article did attempt to solve one limitation of the blockchain infrastructure. OmniPHR attempts to handle the scalability problem. MedRec attempts to handle the mining incentive problem. PSN and the protocols proposed help create a system that handles security of IoT devices. Virtual Resources primarily created a framework to store persistent data storage that is safe, secure, and scalable. Context-driven Data Logging focused on adding a level of confidence to data logging. MeDShare had the goal of adding security and data authentication using blockchain technology and was able to add a level of security to the medical data sharing process, but at the cost of added latency for cloud-based services during high traffic times. Trial and Precision Medicine has the goal of adding integrity and data access security to medical data with a focus on clinical data. Healthcare Data Gateways is a Smartphone (IoT) application that hopes to use the decentralized nature of blockchain technology to add a level of security and data integrity while making legal and regulatory issues easier to manage and give control of data ownership and who can see or not see data to the patient.

Other major problems of healthcare data that are not addressed include interoperability and security, and blockchain struggles to solve some specific challenges in the healthcare arena. Healthcare data is critical for medical practitioners (e.g. physicians and surgeons) to act on in a crisis situation, such as an accident resulting in a patient being presented in the operating room. In such cases, many of the blockchain experiments proposed in this paper would be ineffective and dangerous for a patient as it requires a patient to specifically authorize the transfer of a record. This is clearly impractical, when the patient is not in a state to give consent (e.g. unconscious or suffering a heart attack). In the case when a patient would be unable to share or authorize these records such as a surgeon in an emergency room needing their data to perform a surgery, the patient would not be able to share their records. Many of the solutions proposed seem to prefer a unrealistic scenario, where patient data is controlled by patients who have foresight on their conditions and can make the appropriate decisions ahead of time. Another major challenge not addressed is key management and key leakage. In the case that a key is lost, which might be commonplace among patients or the elderly, how can the data be recovered or authenticated is a lingering question. A secondary method of recovering the patient data needs to be addressed for a real-world deployment of the technology.

The conclusion and future work section will be introduced in the next section.

6. Conclusion and Future Work

In conclusion, blockchain technology has potential applications to some of the challenges faced by the healthcare industry. The strongest potential of blockchain technology in the healthcare arena is its heavily researched applications, namely: security, integrity, decentralized nature, availability, and authentication principles due to the general ledger and block related infrastructure. The healthcare industry is facing issues adapting to a growing technological infrastructure focused on Internet enabled devices, IoT, smart devices, and sensing devices. As such technologies enable the healthcare industry to better serve its patients in an every growing interconnected world, malicious actors can also exploit vulnerabilities in these technologies (as well as processes and users) to access and duplicate the data, make it harder to share records between hospitals. This can result in outdated data, and consequently health problems or misdiagnosis, and a problem verifying a patient's identity. Based on the literature surveyed in this paper, there is clear potential for blockchain technology to be used to address a number of existing issues in the healthcare sector. Existing applications focus on issues of authentication, integrity, record sharing, interoperability, IoT security, edge host security, and patient empowerment. The goal is to make patients have

control and ownership of their medical data sharing and letting who they want to see the data see the data in a secure environment.

Even with these clear improvements to medical applications and smartphone applications, there are still clear security challenges, as blockchain is not without its potential problems. Healthcare and any other industry that wants to use blockchain enabled devices needs to continue education in these areas to help improve and create a strong ecosystem, which can be used to create a better patient centered data empowerment age. Potential research agenda include the following:

1. Research is needed to focus on specific blockchain related issues and attacks such as a block withholding attack and blockchain mining incentives.

2. Research is needed in the area of blockchain enabled healthcare scalability. Scalability is a major issue as healthcare is a growing industry, particularly as our society greys. Blockchain enabled applications will become exponentially harder to run with the number of members or patients on the system increases.

3. Further research needs to be conducted with real-world datasets that are open-source to allow other researchers to verify results and dissimenate findings. Many experiments focused on proof-of-concept and we should explore collaboration opportunities between healthcare organizations and researchers to use real-world healthcare data to evaluate the proposed systems (e.g. security, performance, scalability, and other essential properties such as privacy-preserving).

4. Additional research should also focused on key management and security, as well as the capability to easily replace lost or compromised keys.
5. Research also needs to be focused in the realm of identity verification. Many of the experiments focused on having the patient being able to authorize access to patient records beforehand, but in the case of emergency what are backup plans or emergency protocols that can be used to allow a doctor access to the records without authorization.

It is clear that blockchain has many benefits, which can be applied to the healthcare industry to solve different problems in record sharing and security. However, blockchain is not a solution that can be forced into any situation. Instead, careful examination of specific blockchain issues and how they effect the healthcare industry need to be evaluated. Issues such as mining incentives, which are a core mechanism of blockchain have not been fully considered in the healthcare industry, as well as specific blockchain attacks that can halt the entire system.

References

[1] Zheng, Z., et al. *An overview of blockchain technology: Architecture, consensus, and future trends*. in *Big Data (BigData Congress), 2017 IEEE International Congress on*. 2017. IEEE. DOI: 10.1109/BigDataCongress.2017.85.

[2] Zhao, H., et al. *Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys*. in *Autonomous Decentralized System (ISADS), 2017 IEEE 13th International Symposium on*. 2017. IEEE. DOI: 10.1109/ISADS.2017.22.

[3] Ølnes, S., J. Ubacht, and M. Janssen, *Blockchain in government: Benefits and implications of distributed ledger technology for information sharing*. 2017, Elsevier.

[4] Sullivan, C. and E. Burger, *E-residency and blockchain.* Computer Law & Security Review, 2017. Volume 33, Issue 4, August 2017, p. 470-481.

[5] Mansfield-Devine, S., *Beyond Bitcoin: using blockchain technology to provide assurance in the commercial world.* Computer Fraud & Security, 2017. **2017**(5): p. 14-18.

[6] Beninger, P. and M.A. Ibara, *Pharmacovigilance and biomedical informatics: a model for future development*. Clinical therapeutics, 2016. **38**(12): p. 2514-2525.

[7] Kshetri, N., *Blockchain's roles in strengthening cybersecurity and protecting privacy.* Telecommunications Policy, 2017. Volume 41, Issue 10, November 2017, p. 1027-1038.

[8] Au, M.H., et al., *A general framework for secure sharing of personal health records in cloud system.* Journal of Computer and System Sciences, 2017. DOI: 10.1016/j.jcss.2017.03.002.

[9] Yüksel, B., A. Küpçü, and Ö. Özkasap, *Research issues for privacy and security of electronic health services.* Future Generation Computer Systems, 2017. **68**: p. 1-13.

[10] Roehrs, A., C.A. da Costa, and R. da Rosa Righi, *OmniPHR: A Distributed Architecture Model to Integrate Personal Health Records.* Journal of Biomedical Informatics, 2017. DOI: 10.1016/j.jbi.2017.05.012.

[11] Azaria, A., et al. *Medrec: Using blockchain for medical data access and permission management*. in *Open and Big Data (OBD), International Conference on*. 2016. IEEE. DOI: 10.1109/OBD.2016.11.

[12] Mettler, M. *Blockchain technology in healthcare: The revolution starts here*. in *e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on*. 2016. IEEE. DOI: 10.1109/HealthCom.2016.7749510.

[13] Zhang, J., N. Xue, and X. Huang, *A Secure System For Pervasive Social Network-Based Healthcare.* IEEE Access, 2016. **4**: p. 9239-9250.

[14] Torre, I., et al. *A framework for personal data protection in the iot*. in *Internet Technology and Secured Transactions (ICITST), 2016 11th International Conference for*. 2016. IEEE. DOI: 10.1109/ICITST.2016.7856735.

[15] Samaniego, M. and R. Deters. *Hosting virtual IoT resources on edge-hosts with blockchain*. in *Computer and Information Technology (CIT), 2016 IEEE International Conference on*. 2016. IEEE. DOI: 10.1109/CIT.2016.71.

[16] Siddiqi, M., S.T. All, and V. Sivaraman. *Secure lightweight context-driven data logging for bodyworn sensing devices*. in *Digital Forensic and Security (ISDFS), 2017 5th International Symposium on*. 2017. IEEE. DOI: 10.1109/ISDFS.2017.7916500.

[17] Stanciu, A. *Blockchain Based Distributed Control System for Edge Computing*. in *Control Systems and Computer Science (CSCS), 2017 21st International Conference on*. 2017. IEEE. DOI: 10.1109/CSCS.2017.102.

[18] Shae, Z. and J.J. Tsai. *On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine*. in *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. 2017. IEEE. DOI: 10.1109/ICDCS.2017.61.

[19] Xia, Q., et al., *MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain.* IEEE Access, 2017. **5**: p. 14757-14767.

[20] Jin, T., et al. *BlockNDN: A bitcoin blockchain decentralized system over named data networking*. in *Ubiquitous and Future Networks (ICUFN), 2017 Ninth International Conference on*. 2017. IEEE. DOI: 10.1109/ICUFN.2017.7993751.

[21] Suzuki, S. and J. Murai. *Blockchain as an Audit-Able Communication Channel*. in *Computer Software and Applications Conference (COMPSAC), 2017 IEEE 41st Annual*. 2017. IEEE. DOI: 10.1109/COMPSAC.2017.72.

[22] Anjum, A., M. Sporny, and A. Sill, *Blockchain Standards for Compliance and Trust.* IEEE Cloud Computing, 2017. **4**(4): p. 84-90.

[23] Gazali, H.M., et al. *Re-inventing PTPTN study loan with blockchain and smart contracts*. in *Information Technology (ICIT), 2017 8th International Conference on*. 2017. IEEE. DOI: 10.1109/ICITECH.2017.8079940.

[24] Shrestha, A.K. and J. Vassileva. *Towards decentralized data storage in general cloud platform for meta-products*. in *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies*. 2016. ACM p. 1- 7.

[25] Tosh, D.K., et al. *Security implications of blockchain cloud with analysis of block withholding attack*. in *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*. 2017. IEEE Press p. 458-467.

[26] Liang, X., et al. *Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability*. in *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*. 2017. IEEE Press. p. 468-477.

[27] Raju, S., V. Rajesh, and J.S. Deogun. *The Case for a Data Bank: an Institution to Govern Healthcare and Education*. in *Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance*. 2017. ACM. p. 538-539.

[28] Yue, X., et al., *Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control*. Journal of medical systems, 2016. **40**(10): p. 218.

[29] Zhang, Y., M. Chen, and V.C. Leung, *Topical Collection on "Smart and Interactive Healthcare Systems"*. Journal of Medical Systems, 2017. **41**(8): p. 121.

[30] Dubovitskaya, A., et al. *How Blockchain Could Empower eHealth: An Application for Radiation Oncology*. in *VLDB Workshop on Data Management and Analytics for Medicine and Healthcare*. 2017. Springer. DOI: 10.1007/978-3-319-67186-4_1.

[31] Li, X., et al., *A survey on the security of blockchain systems.* Future Generation Computer Systems, 2017. DOI: 10.1016/j.future.2017.08.020.

[32] Tschorsch, F. and B. Scheuermann, *Bitcoin and beyond: A technical survey on decentralized digital currencies.* IEEE Communications Surveys & Tutorials, 2016. **18**(3): p. 2084-2123.

[33] Conoscenti, M., A. Vetro, and J.C. De Martin, *Blockchain for the Internet of Things: a Systematic* in Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of: p. 1-6.

[34] Karafiloski, E. and A. Mishev. *Blockchain solutions for big data challenges: A literature review*. in *Smart Technologies, IEEE EUROCON 2017-17th International Conference on*. 2017. IEEE DOI: 10.1109/EUROCON.2017.8011213.

[35] Sankar, L.S., M. Sindhu, and M. Sethumadhavan. *Survey of consensus protocols on blockchain applications*. in *Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on*. 2017. IEEE. DOI: 10.1109/ICACCS.2017.8014672.

[36] Mukhopadhyay, U., et al. *A brief survey of Cryptocurrency systems*. in *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*. 2016. IEEE. DOI 10.1109/PST.2016.7906988.

[37] "What is a protocol?" *prisma-statement.org*, 2015 retrieved from http://www.prisma-statement.org/Protocols/Default.aspx [Last access February, 2, 2018].

[38] Kiyomoto, S., M.S. Rahman, and A. Basu. *On blockchain-based anonymized dataset distribution platform*. in *Software Engineering Research, Management and Applications (SERA), 2017 IEEE 15th International Conference on*. 2017. IEEE. DOI: 10.1109/SERA.2017.7965711.

[39] Cai, Y. and D. Zhu, *Fraud detections for online businesses: a perspective from blockchain technology.* Financial Innovation, 2016. **2**(1): p. 20.

[40] Xu, J.J., *Are blockchains immune to all malicious attacks?* Financial Innovation, 2016. **2**(1): p. 25.

[41] Zhu, H. and Z.Z. Zhou, *Analysis and outlook of applications of blockchain technology to equity crowdfunding in China.* Financial Innovation, 2016. **2**(1): p. 29.

[42] Hou, H. *The Application of Blockchain Technology in E-Government in China*. in *Computer Communication and Networks (ICCCN), 2017 26th International Conference on*. 2017. IEEE. DOI: 10.1109/ICCCN.2017.8038519.

[43] Pokrovskaia, N. *Tax, financial and social regulatory mechanisms within the knowledge-driven economy. Blockchain algorithms and fog computing for the efficient regulation*. in *Soft Computing and Measurements (SCM), 2017 XX IEEE International Conference on*. 2017. IEEE. DOI: 10.1109/SCM.2017.7970698.

[44] Dorri, A., S.S. Kanhere, and R. Jurdak. *Towards an Optimized BlockChain for IoT*. in *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*. 2017. ACM. p. 173-178.

[45] Natoli, C. and V. Gramoli. *The Balance Attack or Why Forkable Blockchains Are Ill-Suited for Consortium*. in *Dependable Systems and Networks (DSN), 2017 47th Annual IEEE/IFIP International Conference on*. 2017. IEEE. DOI: 10.1109/DSN.2017.44.

[46] Morabito, V., *Blockchain and Enterprise Systems*, in *Business Innovation Through Blockchain*. 2017, Springer. p. 125-142.

[47] Jiang, P., et al., *Searchain: Blockchain-based private keyword search in decentralized storage.* Future Generation Computer Systems, 2017. DOI: 10.1016/j.future.2017.08.036.

[48] Abouelmehdi, K., et al., *Big data security and privacy in healthcare: A Review*. Procedia Computer Science, 2017. **113**: p. 73-80.

[49] Small, A. and D. Wainwright, *Privacy and security of electronic patient records–Tailoring multimethodology to explore the socio-political problems associated with Role Based Access Control systems*. European Journal of Operational Research, 2017. Volume 265, Issue 1, 16 February 2018, p. 344-360.

[50] Khan, S.I. and A.S.L. Hoque. *Privacy and security problems of national health data warehouse: a convenient solution for developing countries*. in *Networking Systems and Security (NSysS), 2016 International Conference on*. 2016. IEEE. DOI: 10.1109/NSysS.2016.7400708.

[51] Tseng, T.-W., C.-Y. Yang, and C.-T. Liu. *Designing Privacy Information Protection of Electronic Medical Records*. in *Computational Science and Computational Intelligence (CSCI), 2016 International Conference on*. 2016. IEEE. DOI: 10.1109/CSCI.2016.0022.

[52] Vithanwattana, N., G. Mapp, and C. George. *mHealth-Investigating an information security framework for mHealth data: Challenges and possible solutions*. in *Intelligent Environments (IE), 2016 12th International Conference on*. 2016. IEEE. DOI: 10.1109/IE.2016.59.

[53] Kotz, D., et al., *Privacy and security in mobile health: a research agenda.* Computer, 2016. **49**(6): p. 22-30.

[54] Sahi, M.A., et al., *Privacy Preservation in e-Healthcare Environments: A Review.* IEEE Access, 2017. DOI: 10.1109/ACCESS.2017.2767561.

[55] Jain, P., M. Gyanchandani, and N. Khare, *Big data privacy: a technological perspective and review.* Journal of Big Data, 2016. **3**(1): p. 25.

[56] Al-Janabi, S., et al., *Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications.* Egyptian Informatics Journal, 2017. **18**(2): p. 113-122.

[57] Mohan, P. and M. Singh, *Security Policies for Intelligent Health Care Environment.* Procedia Computer Science, 2016. **92**: p. 161-167.

[58] Al-Muhtadi, J., et al., *Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment.* Health Informatics Journal, 2017: p. 1460458217706184.

[59] Al Ameen, M., J. Liu, and K. Kwak, *Security and privacy issues in wireless sensor networks for healthcare applications.* Journal of medical systems, 2012. **36**(1): p. 93-101.

[60] Li, H., et al., *Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective.* International journal of medical informatics, 2016. **88**: p. 8-17.

[61] Theoharidou, M., N. Tsalis, and D. Gritzalis, *Smart Home Solutions: Privacy Issues.* Handbook of Smart Homes, Health Care and Well-Being, 2017: p. 67-81.

[62] Ding, D., M. Conti, and A. Solanas. *A smart health application and its related privacy issues*. in *Smart City Security and Privacy Workshop (SCSP-W), 2016*. 2016. IEEE. DOI: 10.1109/SCSPW.2016.7509558.

[63] Fernando, R., et al. *Consumer Oriented Privacy Preserving Access Control for Electronic Health Records in the Cloud*. in *Cloud Computing (CLOUD), 2016 IEEE 9th International Conference on*. 2016. IEEE. DOI: 10.1109/CLOUD.2016.0086.

[64] Sajid, A. and H. Abbas, *Data privacy in cloud-assisted healthcare systems: state of the art and future challenges.* Journal of medical systems, 2016. **40**(6): Article 155.

[65] Dinev, T., et al., *Individuals' Attitudes Towards Electronic Health Records: A Privacy Calculus Perspective*, in *Advances in Healthcare Informatics and Analytics*. 2016, Springer. p. 19-50.

[66] Sinha, S.R. and Y. Park, *Dealing with Security, Privacy, Access Control, and Compliance*, in *Building an Effective IoT Ecosystem for Your Business*. 2017, Springer. p. 155-176.

[67] Sangpetch, O. and A. Sangpetch. *Security Context Framework for Distributed Healthcare IoT Platform*. in *International Conference on IoT Technologies for HealthCare*. 2016. Springer. p. 71-76.

[68] "What is a protocol?" *prisma-statement.org*, 2015 retrieved from http://www.prisma-statement.org/Protocols/Default.aspx [Last access February, 2, 2018].

[69] Andrea Peterson. Yes, terrorists could have hacked Dick Cheney's heart. Washington Post October 21. https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/ [last accessed January 25, 2018].

[70] Mohammad Jabed Morshed Chowdhury, Alan Colman, Muhammad Ashad Kabir, Jun Han, and Paul Sarda. Blockchain versus Database: A Critical Analysis. In Proceedings of 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering, pp. 1348 – 1353, 2018.

[71] Xu Wang, Xuan Zha, Wei Ni, Ren Ping Liu, Y. Jay Guo, Xinxin Niu, and Kangfeng Zheng. Survey on blockchain for Internet of Things. Computer Communications, 2019. 136: 10-29

[72] Edward C. Cheng, Ying Le, Jia Zhou and Yang Lu. Healthcare services across China – on implementing an extensible universally unique patient identifier system. International Journal of Healthcare Management, **2018**, 11(3): 210–216

[73] Paul J Taylor, Tooska Dargahi, Ali Dehghantanha, Reza M. Parizi, and Kim-Kwang Raymond Choo. A Systematic Literature Review of Blockchain Cyber Security. Digital Communications and Networks, **2019**.

Thomas McGhin is a cyber security graduate from The University of Texas at San Antonio, and his research interests are mainly in cyber security.

Kim-Kwang Raymond Choo holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio. In 2016, he was named the Cybersecurity Educator of the Year - APAC (Cybersecurity Excellence Awards are produced in cooperation with the Information Security Community on LinkedIn), and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008. He is also a Fellow of the Australian Computer Society, an IEEE Senior Member, and the Co-Chair of IEEE Multimedia Communications Technical Committee (MMTC)'s Digital Rights Management for Multimedia Interest Group.

Charles Zhechao Liu received his Ph.D. in management information systems from the University of Pittsburgh. He is currently an Associate Professor at The University of Texas at San Antonio. His current research interests include the economics of information systems and cyber security, mobile apps, and data analytics. Dr. Liu is an International Conference on Information Systems (ICIS) Doctoral Consortium Fellow and a recipient of the Net Institute Research Grant and the 2018 UTSA College of Business Dean's Distinguished Research Award. His research has been published in MIS Quarterly, Information Systems Research, Journal of Management Information Systems, Communications of the ACM, Communications of the AIS, etc.

Debiao He received his Ph.D. degree in applied mathematics from School of Mathematics and Statistics, Wuhan University in 2009. He is currently a Professor of the State Key Lab of Software Engineering, Computer School, Wuhan University. His main research interests include cryptography and information security, in particular, cryptographic protocols.