Blockchain and Big Data to Transform the Healthcare

Md Zakirul Alam Bhuiyan
Department of Computer and Information Sciences, Fordham University, NY, USA
mbhuiyan3@fordham.edu

Aliuz Zaman
Department of Computer and Information Sciences, Fordham University, NY, USA

Tian Wang
Department of Computer Science and Technology, Huaqiao University, Fujian 361021, China

Guojun Wang
School of Computer Science and Educational Software, Guangzhou University, Guangzhou 510006, China

Hai Tao
School of Computer Science, Baoji University of Art and Science, Shaanxi, China

Mohammad Mehedi Hassan
Information Systems Department, King Saud University, Riyadh, Saudi Arabia

ABSTRACT

The increase in reported incidents of security breaches that compromise privacy of individuals requires us to question the current model used to collect patient information. What we have learned from bitcoin and the underlying blockchain technology is that there are ways for us to protect this information by using a distributed ledger. In this paper, we review and propose a solution that can be used to manage individual health data as well as cross-institutional sharing of this information. The solution will increase clinical effectiveness and an increase in research when the data is shared with researchers. The proposed system solution based on blockchain technology that includes providers, hospitals and clinic, insurance companies, and patients. All along the ownership of the data would belong to the individual or the patient. In the solution, we suggest to adopt a private blockchain solution where all participants are known and trusted, which allows for privacy and security of the data.

CCS Concepts

Information systems → Information systems applications → Decision support systems → Data analytics

Keywords

Blockchain; big data; healthcare: patent data: privacy

1. INTRODUCTION

Big data refers to massive volume of structured and unstructured data so large that it is difficult to process using traditional database or software techniques. In healthcare, data is being generated continuously, every time we visit our primary care physician or a specialist, every trip to an emergency room (ER) or any surgical procedures that we undergo. In addition, now with the availability of wearables and other IoT devices, the amount of data being generated is multiplying fast. Then, there are insurance companies that use the data submitted by the healthcare providers to pay them for their services. This data comes in different forms; unlike old days this is not just basic patient information [1-4].

We have all experienced how every doctor we visit has a file full of information about us. They make us sign a piece of paper acknowledging our understanding of their privacy policy, yet when it comes to protecting our data they are not up to par. We have heard of several well know breaches where patient information has been stolen or lost [5-7]. Health information is something hackers look for therefore it is very important to protect this data. Failure to protect patient records can have serious financial and legal consequences and it can impact patient care. Implementing the proper security can be quite expensive, and this could lead to improper security measures in place.

Medical record ownership and sharing of information is another controversial issue. Medical records come in many forms, reports, images, videos and data, this data can be in structure or unstructured form. They could also come in different format depending on the system in use by a given provider thus raising compatibility issues. All patient records are owned by the doctors; they have the right to not share the information with anyone including the patient. The integrity of the documents that are generated is also a major concern, how can we know that data entered in our file has not been changed, removed or destroyed. Sometimes, it is important that a specialist get access to a patients' medical record. Getting access to such an information, in time without delay could be a matter of life and death. The patient records should be consistent and available across institutional boundaries, and the access to this information should be controlled by the patient [8], [9].

In this paper, we review and propose two solutions that can be used to manage individual health data as well as cross-institutional sharing of this information. The solution will increase clinical effectiveness and an increase in research when the data is shared with researchers. The proposed system solution based on blockchain technology that includes providers, hospitals and clinic, insurance companies, and patients. We make certain assumptions for the solution [10]-[12]. First, each of the participants in this peer-to-peer network will find a value in receiving data from other nodes. Second, the security and auditability of the information is understood by all parties so they are willing to share the information, and lastly, the patient controls who has access to this information and when.

If we ask anyone, there are always issues related to medical record access, payment to healthcare providers or trying to find out if a

ICDPA 2018, May 12–14, 2018, Guangdong, China

ACM ISBN 978-1-4503-6418-8/18/05…$15.00
DOI: http:// doi.org/10.1145/3224207.3224220

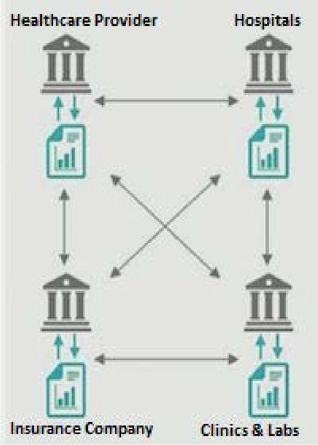

Figure 1. Participants in the healthcare blockchain.

patient is covered by insurance when the service is provided. All these issues can be covered by implementing a distributed peer-to-peer network based on the blockchain technology. Our motivation behind this paper is to provide the solution using blockchain that would allow different participants in the healthcare to come together and share data which will not only reduce cost but also provide many other benefits, such as, efficiency in care delivery for the patient where multiple providers can share data that they currently have in silos within their own medical records systems, as shown in Fig. 1.

Organizations spend a considerable amount of time and money to set up information systems and data exchanges, that requires continuous maintenance, and data backups. To share information among participants they have to extract information then transfer it to the requesting entity, which can be time consuming and expensive. Our proposed solution can help. The solution using blockchain technology that includes providers, hospitals and clinic, insurance companies, and patients. All along the ownership of the data would belong to the individual or the patient. In the solution, we suggest to adopt a private blockchain solution where all participants are known and trusted, which allows for privacy and security of the data [4].

The rest of the paper is as follows. Section 2 describes blockchain and big data in health care. Section 3 offers healthcare data security and privacy. Section 4 explains blockchain for healthcare privacy and security. Section 5 provides the blockchain solutions. Finally, Section 6 conclude the paper.

2. BLOCKCHAIR AND BIG DATA IN HEALTHCARE

2.1 The Blockchain Technologies

A block in blockchain is a set of information that has been committed together as a transaction. Several these blocks are linked together to form a blockchain. As the number of transactions increases, the size of the blockchain increases. The first chain of a block chain is called the genesis chain. Each block is comprised of a hash that acts like a digital finger print and uniquely identifies the transaction. It also includes a hash to the prior block. The genesis block is the only block that does not have a pointer to the previous block, as shown in Fig. 2 [13], [14].

The hash to the prior block acts as a safeguard for the contents of the block. If the contents are updated in any way, the hash cannot be verified and this indicates evidence of data tampering. This tamper-proofing is what gives the data in a blockchain immutability, i.e., data within a block can never be modified.

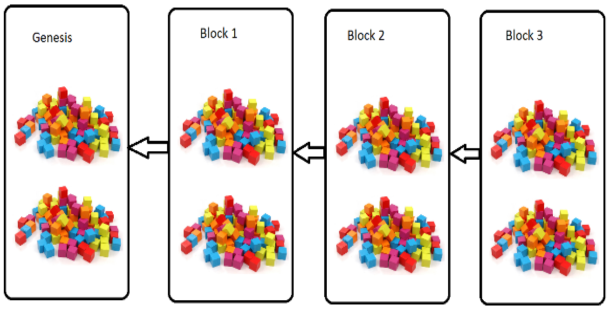

Figure 2. Example of a blockchain.

2.1.1 Blockchain features

There are several features from the blockchain technologies.

a) Shared Ledger. The purpose of a ledger is to create an immutable record of all transactions, that all participants can access. The shared ledger is the single source of truth. Through replication, each participant has a copy of the ledger. The ledger can be permissioned such that each user is only authorized to see the content that they have been given access to.

b) Permission. A blockchain can have permissions assigned to it. With permissioned blockchains, each user has a digital identity that which policies around their permissions to be used, that allow selective access to transaction details. This allows organizations to comply with data protection regulations such as HIPAA. For example, in a counterparty transaction, both parties can see the details of the transaction. An independent entity can see that the transaction has occurred, but is not able to view details. If an auditor joins the network they can be setup using digital certificates, such that, they see details of the transaction. A digital certificate helps establish identity of the user or party and the blockchain network can be setup to work with a certification authority that can verify this certificate.

c) Consensus. A consensus algorithm helps ensure that the next block in the chain is the one and only truth, and it prevents other powerful parties from forking the chain and tampering with data. Consensus is necessary to determine if the transaction is permanently incorporated into the blockchain. There are four consensus algorithms:

i. Practical Byzantine Fault Tolerance.
ii. Proof of Work.
iii. Proof of Stake.
iv. Delegated Proof of Stake.

d) Smart Contracts. A smart contract is an agreement or set of rules that govern a business transaction; it’s stored on the blockchain and is executed automatically as part of a transaction. For example, let’s assume that a pizza company makes a promise to deliver our pizza within 30 minutes. A smart contract can be set such that if the delivery does not happen in 30 minutes, the blockchain releases a partial refund. These sorts of contracts are particularly useful for instances such as financial contracts that require payments to be settled by a certain date or for automatic payouts of travel insurance, such as when a flight is delayed by more than the maximum allowed delay time.

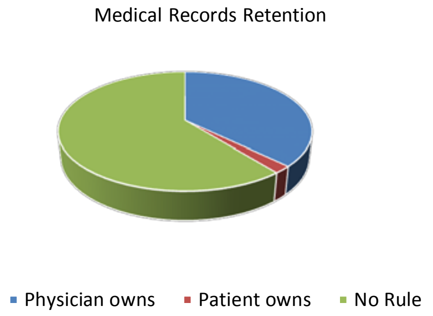

Figure 3. Medical records retention and access laws.

2.1.2 Types of blockchain

While the Blockchain model was originally created for the bitcoin currency, several new and unintended industries have started to see the potential of blockchain. The constraints imposed by the public bitcoin model adopted by bitcoin may not be necessary or in some way hinder adoption for several different sectors. Depending on the need and business model there are diverse types of blockchains that could be used. Two main types are public blockchain and private blockchain.

2.1.3 Consortium

A consortium blockchain is sort of a middle-ground between completely private and public blockchains. It is a hybrid, that is neither as low-trust as a public blockchain and neither does it have the overarching highly-trusted entity model of a private blockchain. A consortium platform provides some of the benefits of private blockchains such as privacy and efficiency, without giving control to just one company. A consortium platform provides some of the benefits of private blockchains such as privacy and efficiency, without giving control to just one company. A consortium usually operates under the guidance of a group that oversees it.

2.1.4 Big Data in healthcare

There are big changes taking place in healthcare when it comes to big data, the amount of information being gathered has increased in the past few years. Also, technical advances have made it much easier to collect and analyze data from multiple sources like, insurance carriers, hospitals, laboratories and physicians' offices. Traditionally, physicians used their judgement in making treatment decisions, however, this has changed in recent years to a more evidence-based medicine. This new approach involves reviewing clinical data and making treatment decisions on the best available information. Healthcare sector has lagged behind other sectors like banking and retail when it comes to use of big data.

Big data in healthcare is being used to predict epidemics, cure disease, improve quality of life and avoid preventable deaths. Recently, we have had a lot of wearable devices that have hit the market like Fitbit, Samsung Gear Fit and Jawbone, these allow us to track our progress. Soon, we will be able to share this information with our doctor, who will be able to use it as part of their diagnostic process when we visit him with an ailment. As more and more data is collected, doctors will be able to give treatment options based on the data from other patients with similar conditions, genetic factors and lifestyle. Currently, the big data is stored in siloes within different doctor's computer systems, hospitals, and clinics. In the future, to make a productive use of all this data, it has to be shared with others [2], [3].

3. HEALTHCARE DATA SECURITY AND PRIVACY

Who owns a patient's medical record, is it the doctor or the patient? Doctors say that records represent their medical opinions about the patient and therefore it is not the property of the patient. However, the record is about the patient, the lab work is important information about the patient, why should someone else own that? Who owns a patient's medical record, is it the doctor or the patient? Doctors say that records represent their medical opinions about the patient and therefore it is not the property of the patient. However, the record is about the patient, the lab work is important information about the patient, why should someone else own that?

Different states of the US have different laws regarding ownership; only one state, New Hampshire, explicitly gives ownership to patients, 19 states give hospitals or physicians the ownership of a patient's healthcare data, and 31 states have no law delineating custody of records. In Utah, the physician and/or hospital owns the record, meaning that a patient must go through a hospital medical records department, quite often with considerable delay, to get their own information. Many systems provide limited access to information through web portals [1], [5], [7].

Every year the information stored in healthcare systems increases exponentially, as an enormous amount of information is being collected. All this information can bring unwanted attention. Cybercrime is a massive social and political issue; new breaches are discovered or reported almost daily. The financial and reputational costs associated with these breaches are also massive to the government, healthcare organizations, and patients. Both the private and public sector are dealing with data security challenges. There have been several highly visible private attacks on healthcare providers, like Community Health Services, Advocate Medical Group, and recently with health insurer Anthem Blue Cross and Blue Shield.

No one is clear about the true effects of the HIPAA Privacy Rule, has it strengthened individual privacy rights, maybe, but we are pretty sure that it has increased the awareness on the importance of health information privacy and the role a patient plays in that process. As patients, we have privacy rights when it comes to our own health information and an expectation that our information will be held in confidence and protected.

4. BLOCKCHAIN FOR HEALTHCARE PRIVACY AND SECURITY

The Blockchain technology allows us to organize data in a way that transactions can be verified and recorded while getting consensus from all parties involved, as shown in Fig. 3. The technology uses a concept of authoritative ledger that keeps track of all events. Current ledger systems hold data in a single, centralized location, an Electronic Health Record system, a data warehouse, or a repository run by a health information exchange. Quite often each of these systems are developed independently and might generate and store the data in its own proprietary format, this leads to data siloes and interoperability issues that frustrate providers, patients, and researchers. A Blockchain on the other hand requires each individual participant, or node to hold a copy of the record. Whenever a change is made, it must be compared against each and every node and has to be approved, this increases the security and reduces the likelihood of someone making any unauthorized change [8].

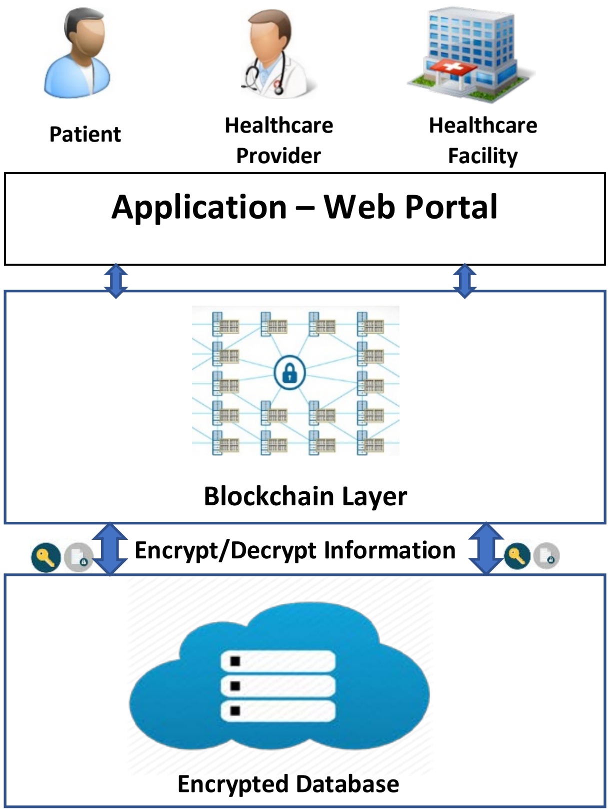

Figure 4. Three-tier solution.

Blockchain will provide the necessary validation the healthcare industry is looking for, and it is something that can be trusted by all parties. As part of the process, one entity is in charge of holding the data, but all who participate in the blockchain are responsible for making sure of the integrity. Unlike a public financial Blockchain the healthcare Blockchain would have to be limited to the number of authorized participants to a patient, the health care provider, healthcare facilities, and the family if needed. This way of collaborating will eliminate many issues faced by the health care industry, because there are no middlemen who are in-charge of the data.

With the Blockchain approach sharing a patient's record cause no trust issues, this is because each participant is known in advance and have already been pre-approved.

In addition to all the data standardization issues, the healthcare systems suffer from fundamental issue when it comes to security and privacy. Healthcare data is personal and private in nature, at present this collection of information is stored in one central location. We can compare it to a bank vault, where access is restricted to those who are trusted and has the key to unlock and access the information. Unfortunately, once someone gains access to the key, that data is theirs for the taking. We have seen an increase in unauthorized users accessing protected health information; this shows us that the way the healthcare stores, shares, and secures its data is in needs a complete overhaul. The blockchain is the technology behind the Bitcoin ecosystem, and it might be the solution to all the security and privacy issues in healthcare. Private and hybrid blockchains would address the privacy, security and scalability concerns. However, how do we decide on which type of blockchain to use, Fig. 4 below shows the questions to ask and how to make an educated decision on choosing the correct blockchain technology. With the blockchain, each member who is part of the hybrid setup will have their own copy of the ledger instead of the data being held in one centralized location. No new transaction can be approved unless a majority of the nodes that are part of blockchain agrees that the requested action is indeed accurate.

Transactions could include anything from monetary payments to an update to a patient's health record. Every new action is verified against an authoritative ledger of previous events. Currently, different healthcare providers have their own versions of a patient's record and these records are never validated against each another. A patient who visits four different providers will have four different sets of records, these records could have errors and the patient is never aware of it because they do not have access to it. With blockchain a patient can have a view into the information that is stored about them in the healthcare system, thus allowing them to modify anything that is incorrect. It also introduces multiple checkpoints rather than one single source for sensitive data which also improves security. Blockchain technology will also have a big impact on the security of healthcare data.

Patients who are part of the blockchain will now be able to control who can access and modify their data, because they will be able to approve or deny access. This will help to ensure a higher level of privacy and transfer the control to those who the data belong to, in this case the patient. Health information exchanges operate in a similar manner, where they use a decentralized approach to their data architecture, however, it is the validation aspect that sets the blockchain technology apart from all others. Now Patients and providers cannot verify that the information transferred between hospitals and other organizations is correct. However, a blockchain participants will know for sure that the information has undergone validation.

Another benefit is that patients do not have to take the time to gather their own records from multiple providers if they must see a new specialist. With blockchain, the new specialist can be given access to the chain. After that, he or she can access the same information as everyone else who is already participating. Patient can finally benefit from the idea that there is, a readily available source of information that can be instantaneously shared among stakeholders and does not require manual data reconciliation.

5. BLOCKCHAIN SOLUTIONS

5.1 Fast Healthcare Interoperability Resources

Fast Healthcare Interoperability Resources (FHIR) [15] is an emerging standard that provides data formats and elements along with publicly accessible APIs that can assist in exchanging Electronic Health Records.

We suggest a solution for FHIR, as shown in Fig. 4, that can be licensed without restrictions or royalty, this should help facilitate a broader adoption of this standard. It will push the increased utilization of mobile and cloud-based applications, medical device integration, and flexible healthcare workflow. FHIR allows the separation of Electronic Health Records data elements into structured data types called resources. Resources can serve different purpose, it can identify between providers and patients and common clinical activities.

FHIR modules can provide a broad set of data from various sources. Some examples are Clinical contents, medications tracking, diagnostics, and Financial data for billing and claims support. We are using FHIR as the format to exchange information between different participants because it is an emerging standard and it provides a chronological record of ownership and origin, in addition there are audit trails which makes it suitable for use in blockchain entries.

The three-tire solution as shown in Fig. 4, blockchain is integrated with electronic health records (EHRs). At present, patient information exchange and access is lacking an umbrella solution. Blockchain can unite technology because it already establishes to enable secure transactions. Only those with the cryptographic security keys can do anything with patient private data. An EHR system can have 3 modes with which information can be shared. The first mode is called "push." Push is basically the sharing data from one health provider to another provider. A health care provider utilize an email client called Direct. However, this way faces challenges. Think that we travel to a new place or a village that does not have a healthcare provider in the network. If we get an urgent, our health information is stranded at our former hospital until that the hospital agrees to release of information, however, we require it immediately Another situation is that there is no assurance that the data will maintain its integrity. We are also aware of the email security issues [16].

The second mode is "pull." If we move to the new hospital in the new place, and they can ask for a request to pull our health data from the hospital where we have the data. However, it is not that easy. Whether or not the new hospital can get the data totally relies on their communication with the previous hospital; there would not be a standardized permission procedure. The third mode is "view." In our health provider network, numerous clinicians and staffs may see our data, however the security measures for transferring data are not standardized. In other ways, one hospital staff could merely utilize gmail to transfer our health data to another hospital. A cyber hacker may hack into a hospital's account and request the data without providing proof of identity or certificate.

The solution in Fig. 4 using blockchain may provide a means through which the healthcare community could resolve all standardization and security issues. All of our data can be available on the blockchain, with a clear trail as to who recorded it, when they recorded it, and other related data. We can be in charge of approving access control to each health provider. Basically, health providers should not have to be the distributors of health data as they are currently, facilitating input, transfer, and access control on a case-by-case basis. As an alternative, each health provider can only input ongoing records into their health database, which in turn can be able to connect that data onto the secure blockchain ledger. Then, we can authorize access.

At the outset, blockchain EHR will simply make it easier for providers across the board to follow HIPAA and access accurate information about our history right away. When we are faced with an emergency, we do not want to wait to access information about our medical history that could save our life. With blockchain, we would not have to.

5.2 Smart Contracts

Smart contract is a term used to describe computer program code that is capable of facilitating, executing, and enforcing the negotiation or performance of an agreement using the blockchain technology. The entire process is automated and can act as a complement, or substitute a legal paper contract.

We propose a solution as shown for patent record keeping, as shown in Fig. 3. In our solution, we will use smart contracts in several ways, they will be used to control access to records, limit who can and cannot access the information, grant and revoke access based on certain conditions. They can be used to automate the agreement between providers, patients and insurance company to share coverage and payment information.

5.3 Transaction-wise Healthcare Blockchain

Our solution uses the blockchain technology to create a trusted distributed system that can securely store an individual's healthcare information. The individual user can manage the permission to their data via a web portal, along with other important functionality such as reviewing logs to see who accessed their information. This will give the individual control over privacy and security over their own sensitive data because they are managing it instead of a third party. They can also provide access to third party as needed.

Choosing a blockchain platform is not an easy task because of the many available options. The application we are suggesting could be developed on the Ethereum blockchain application platform or The Hyperledger being developed by the Linux Foundation. Hyperledger is a good option because it is aimed at building a distributed ledger without the Proof of Work (PoW) or Proof of Stake (PoS), these terms are explained earlier in the paper. It is also starting to push ahead of other blockchain implementations because of its usability. In this paper, we are not going to get into any one particular solution, but use the general concept of blockchain to explain our ideas.

Our solution consists of 3 distinct layers, as shown in Fig. 4. The first layer would be the application layer, which will be used as an administrative portal for user access provisioning, report generation, etc. The application layer would be the interface to the private implementation of the blockchain. The second layer would consist of the blockchain layer, the network of blockchain nodes can only interact with the application layer, other nodes, a key authoring entity and the database. The key authoring entity is the resources that would generate the public/private key pairs for use in the blockchain. The third would be the encrypted database layer, this is where all the electronic Protected Health Information (ePHI) will be stored.

All medical data would be store in an encrypted database, when a healthcare provider or a healthcare facility creates a medical record, this record would be encrypted and sent to the database for storage. Every time information is saved to the database a pointer to that health record is registered in the blockchain along with unique identifier of the user who generated that record. The patient who is the owner of this information will be notified that a new record was added. This process is not only true for a third party, but the patient themselves can add from wearable sensors and other devices.

The patient would have control over how he or she will share this data and they will have full access to this data regardless of where they are in the world. The user can access a web portal to view who has accessed their blockchain. The portal can also be used to authorize access to any individual who has to view the patient's information. The user will be able to have granular control on who has access to the data and when that privilege expires. When the patient goes to new health care provider, all he has to do is give the new provider access to his healthcare information.

When someone requests data, the database will decrypt the data in storage, it then re-encrypts the data using the requestors public key to protect the data in transit. The person who requested the data can encrypt the information using their private key. A single block in the blockchain is constructed using several key elements related to identification information and the list of transactions being stored. The block content represents data ownership and permissions shared by members of the private blockchain network. Smart contracts are used to log the relationship between the participants and how they are connected to the medical record, along with the permissions to view a document and the data pointers to the database is stored here as well. The block itself does not contain the actual data record. The data pointer can be used to retrieve the actual information from the database.

In our solution, we are using a private blockchain where individual entities such as health care providers, laboratories, hospital, etc. would be nodes in the blockchain, so they can all share data with each other or send information related to a visit made by the individual to one of these providers [17]. The blockchain itself will contain a list of all the health records and data collected throughout a patient's lifetime along with the type of data and the location where this data is located. The transactions in the blocks would contain an identifier that is unique to the user, it will also hold an encrypted link to where the health record is actually stored, type of data contained in the health record and a time stamp of when the transaction took place.

5.4 Advantage of Blockchain over current systems

There are several benefits to the healthcare industry based on our solution. Using blockchain will allow patients, healthcare providers, researchers and others to access accurate information in a timely manner. Currently, there are Electronic Medical Records systems that are centralized, or the data is stored in paper files in the physicians' office. Getting access to this information can take several days if not week. A blockchain solution offers many advantages to healthcare providers, individuals, researchers and others who actively participate in the healthcare industry.

Researchers in healthcare require access to comprehensive medical data in order for them to get a better understanding of diseases, fast track the development of drugs and design treatment plans that are based on a patient's genetic makeup. A blockchain with its de-centralized nature would provide a diverse set of data by including information about patients from different ethnic backgrounds and from diverse geographical environments. It can collect health data across a patient's lifetime. Blockchain could provide real-time access to data, this could improve clinical care coordination and vastly improve clinical care in emergency situation. It will allow researchers and those in public health service to rapidly detect conditions that can impact public health. Epidemics can be detected and contained faster.

The healthcare provider and patients will have access to the same information and they would be able to engage in a collaborative discussion about the best treatment available based on research and not just intuition. This system will help eliminate healthcare breaches, provide a way for facilitated care coordination that will improve overall health outcomes.

6. CONCLUSIONS

The technology provides a promising way to avoid many of the issues that have prevented providers, researchers, and patients from taking full advantage of healthcare's big data, which is growing exponentially each and every year. If the healthcare industry can find a way to integrate this approach they may find that are able to solve many of their problems much faster than expected. The excitement around the technology may imply a certain inevitability, but the challenges and realities of health care and health care data may be insurmountable — even as some argue that blockchain could revolutionize how we share health care data. We need more real-world uses to truly understand how useful blockchain could be, how disruptive implementation would be, and how much is just hype.

7. REFERENCES

[1] "Who Owns Medical Records: 50 State Comparison." 2015. Health Information and the Law. *George Washington University Hirsh Health Law and Policy Program.* Aug. 20, 2015.

[2] M. Bhuiyan, G. Wang, W. Tian, M. Rahman, and J. Wu, Content-Centric Event-Insensitive Big Data Reduction in Internet of Things, *IEEE GLOBECOM 2017*, Singapore, December 4-8, 2017

[3] J. Son, J. Park, H. Oh, M. Bhuiyan, J. Hur, and K. Kang, Privacy-Preserving Electrocardiogram Monitoring for Intelligent Arrhythmia Detection, *Sensors* 2017, 17(6):1-22, 1360, doi:10.3390/s17061360

[4] T. Wang, M. A. Bhuiyan, G. Wang, M. Rahman, J. Wu, and J. Cao, Big Data Reduction for Smart City's Critical Infrastructural Health Monitoring, *IEEE Communication Magazine (COMMAG)*, 56(3): 128 – 133.

[5] M. Bhuiyan, M. Zaman, G. Wang, T. Wang, and J. Wu, Privacy-Protected Data Collection in Wireless Medical Sensor Networks,*" The 12th International Conference on Networking, Architect and Storage (NAS 2017),* August 7- 8, 2017, Shenzhen, China

[6] F. Rahman, M. Bhuiyan, and S. Ahamed, A privacy preserving framework for RFID based healthcare systems," *Future Generation Computer Systems*, 72: 339-352, 2018 2017

[7] E. Luo, M. A. Bhuiyan, G. Wang, M. Rahman, J. Wu, and M. Atiquzzaman, PrivacyProtector: Privacy-Protected Patient Data Collection in IoT-based Healthcare Systems, *IEEE Communication Magazine (COMMAG),* 56(2): 163-168, 2018

[8] M. Kenneth, D. Markwell, R. MacDonald, P. Szolovits, and I. Kohane, 2011. *Public Standards and Patients' Control: how to keep electronic medical records accessible but private.* BMJ 322, no. 7281 (2001): 283-287.

[9] Wood, Gavin. 2014. "Ethereum: A secure decentralised generalised transaction ledger." *Ethereum Project Yellow Paper* (2014).

[10] A. Ekblaw, A. Azaria, J. Halamka, M. Lippman, 2016. A Case Study for Blockchain in Healthcare: MedRec" prototype for electronic health records and medical research data. https://www.media.mit.edu/publications/medrec-whitepaper/

[11] X. Yue1, H. Wang, D. Jin, M. Li, W. Jiang. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *J Med Syst.,* 40(10): 218, 2016.

[12] P. Tak and S. Liu. Medical Record System Using Blockchain, Big Data and Tokenization,"

https://hbr.org/2014/12/why-health-care-may-finally-be-ready-for-big-data

[13] Sonja Zillner and Sabrina Neururer. Big Data in the Health Sector," In: Cavanillas J., Curry E., Wahlster W. (eds) New Horizons for a Data-Driven Economy. Springer, Cham

[14] Miles Price, Blockchain: The Complete Guide to Understanding Blockchain Technology, CreateSpace Independent Publishing Platform, 2017

[15] Fast Healthcare Interoperability Resources (FHIR) https://www.hl7.org/fhir/overview.html

[16] B. Narayanan, Bitcoin and cryptocurrency technologies, *Princeton: Princeton University Press*

[17] T. Tran, M. Rahman, M. Bhuiyan, A. Kubota, S. Kiyomoto, and K. Omote, Optimizing Share Size in Efficient and Robust Secret Sharing Scheme for Big Data," *IEEE Transactions on Big Data*, 2017, DOI: ttps://doi.org/10.1109/TBDATA.2017.27080