HealthCare BlockChain

Ali Fakih 95497 Maria Afara 95492
Fakih.k.ali@gmail.com Maria-afara5@hotmail.com
Supervised by Dr Mohammad Chaito

Contents

Abstract

Blockchain technology is a system of creating an immutable, secure, distributed database of transactions. Blockchains were initially created to provide a distributed ledger of financial transactions that did not rely upon a central bank, Credit Company, or other financial institution. The technological breakthrough, however, has been extended to transactions involving legal matters, medical records, insurance billing, and smart contracts. One primary way that blockchain technology is important to healthcare professionals in that it can revolutionize medical database interoperability. This greater interoperability can help improve access to medical records, imaging archives, prescription databases. Given that a patient's medical history is a primary cornerstone of good medicine, blockchain technology has the potential to dramatically improve medical care.

1. Introduction

Blockchain technology is a system of ensuring a secure, tamper-proof, and permanent record of transactions. The fundamental idea of a distributed secure ledger was invented in 2008 by Satoshi Nakamoto . Initially, the technology created bitcoin, which verifies financial transactions without the requirement for a central authority, the Federal Reserve, a central bank, or other financial institution. Because the method of transaction verification involves a network of computers, rather than a single computer, it is very fault-tolerant. Any single computer can be added or removed from the network at any time without corrupting the ledger of transactions. Because the ledger is duplicated across all network computers, transactions are secure and immutable. A key feature of blockchain technology is that it is trust-less: transactions are processed by the network so there is no need to trust a single computer, database, or institution. The initial blockchain created bitcoin, which consists of a secure, immutable, distributed database of financial transactions. However, the technology has also been extended to create a system of secure, immutable, distributed computer programs allowing the creation of smart contracts and artificial intelligence.

2. Interoperability

Interoperability is the ability to work together in an organized manner. Applied to electronic medical records, interoperability means the ability of large computer databases containing patient information to effectively communicate with each other and ultimately communicate the data to healthcare providers quickly in a meaningful way. Even though the Internet has been transmitting data around the world for almost 50 years now, critically important medical data remains for the most part hidden away tightly in silos, run by hospitals, clinics, and insurance companies. This tight lock on patient records means that even when going a short distance within the same town it is difficult to access medical records from a different clinic. Although the clinic is in the same city, the silo housing medical records is just as isolated as if it was located thousands of miles away. These silos effectively control medical records, instead of the patient controlling their own medical records. Because of the hassle of transferring medical records, many patients will stay within a single healthcare system for the sole reason that their medical records are housed within that system.

3. Case Study

One of the biggest challenges in medicine is inaccessible medical records for acutely ill patients unable to verbalize or recall their personal information. For example, a patient was admitted from the emergency room because of an acute respiratory failure. He could not verbalize his medical history, because all of his focus and efforts were upon getting enough air. In terms of his medical history, his medical team was flying blind. The patient was a 48 year old long haul

truck driver from out of town. No family was at the bedside and no medical records were available. What medications was he on? What allergies did he have? Given all of the unknowns, the patient received the generic, one size fits all treatment for acute hypoxic respiratory failure. Over the next several hours, his heart rate gradually increased into the 130's. Most likely, he was developing sepsis from an acute infection which was the cause of his initial breathing difficulties. In response, he was given antibiotics and intravenous fluids, again the generic treatment for what was the most likely cause of his condition. But it turns out his symptoms were due to something else entirely, that would not have been missed if old medical records had been available. The patient just had a severe exacerbation of his chronic obstructive pulmonary disease. He didn't have sepsis at all. His increased heart rate was due to beta blocker withdrawal from not getting his routine nightly dose of metoprolol. He was eventually discharged from the hospital in good condition, back at his baseline. His hospitalization, however, was prolonged by a full day and he received unnecessary antibiotics all because nobody knew he was on a beta blocker. His old medical records were in Oklahoma, locked up safe and secure in an electronic database. We, however, were in Oregon. While his medical records were secure in Oklahoma, they were not useful. His home clinic's database had no interoperability with the clinical database at the hospital in Oregon. The result was not fatal, however, his hospitalization was prolonged and his diagnosis delayed due to poor computer database to computer database communication.

4. Future Directions

The next major advance in medical records is not going to be a new software program that runs on a database isolated within a single healthcare organization. The next advance will be the creation of a distributed ledger which will effectively transfer control of patient records from the healthcare organization to the individual. When medical records become as freely mobile as people, we will have made a tremendous leap forward in medicine. Blockchain technology is the key scientific breakthrough enabling this major step forward. The process of making the medical records of individuals readily accessible requires the use of distributed databases stored on the cloud in a secure yet open manner. The records must be secure, immutable, and at the same time easily accessible. Blockchain technology is the vehicle that makes all of these goals possible.

5. Underlying Fundamentals of Blockchain Technology

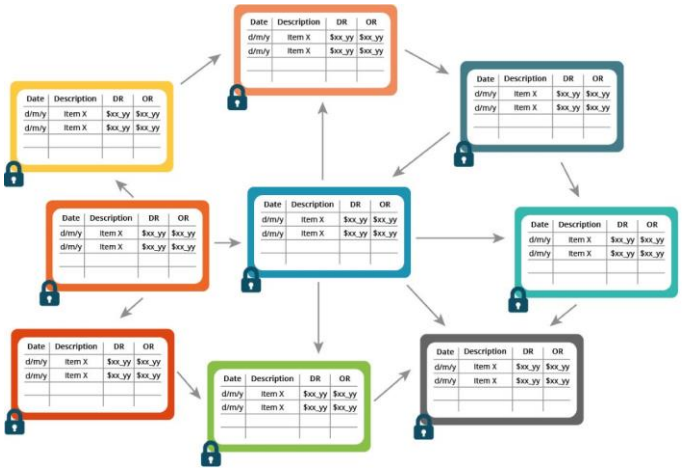
Blockchain is a peer-to-peer (P2P) distributed ledger technology for a new generation of transactional applications that establishes transparency and trust. Blockchain is the underlying fabric for Bitcoin and is a design pattern consisting of three main components: a distributed network, a shared ledger and digital transactions.

a. Distributed Network

Blockchain is a decentralized P2P architecture with nodes consisting of network participants. Each member in the network stores an identical copy of the blockchain and contributes to the collective process of validating and certifying digital transactions for the network.

b. Shared Ledger

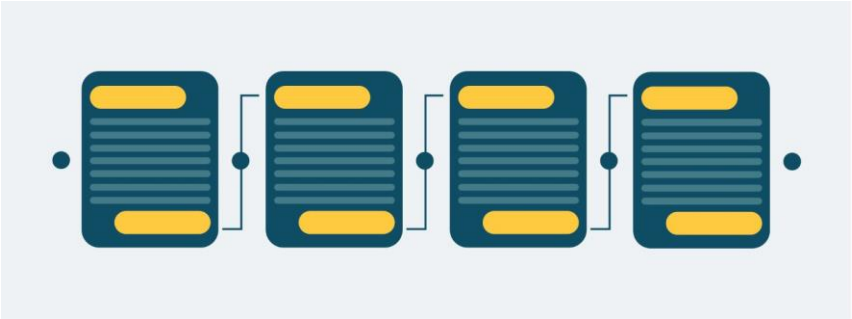
Members in the distributed network record digital transactions into a shared ledger. To add transactions, members in the network run algorithms to evaluate and verify the proposed transaction. If a majority of the members in the network agree that the transaction is valid, the new transaction is added to the shared ledger. Changes to the shared ledger are reflected in all copies of the blockchain in minutes or, in some cases, seconds. After a transaction is added it is immutable and cannot be changed or removed. Since all members in the network have a complete copy of the blockchain no single member has the power to tamper or alter data.



Blockchain is a decentralized P2P architecture. Members in the distributed network record digital transactions into a shared ledger. Each member stores an identical copy of the shared ledger and changes to the shared ledger are reflected in all copies.

c. Digital Transactions

Any type of information or digital asset can be stored in a blockchain, and the network implementing the blockchain defines the type of information contained in the transaction. Information is encrypted and digitally signed to guarantee authenticity and accuracy. Transactions are structured into blocks and each block contains a cryptographic hash to the prior block in the blockchain. Blocks are added in a linear, chronological order.



Transactons contain encrypted and digitally signed data along with an index that points to the prior block in the blockchain. Transactions are structured into blocks and recorded in chronological order.

6. Bitcoin and Private Blockchain Limitations for Health Care Application

Bitcoin is based on open-source cryptographic protocols and has proven to be a very safe platform for crypto-currency exchange. While the identities behind some Bitcoin transactions remain unknown, the platform provides transparency as anyone can access the blockchain and see balances and transactions for any Bitcoin address.

Lack of data privacy and the absence of robust security make the Bitcoin public blockchain unsuitable for a health blockchain that requires privacy and controlled, auditable access. Additionally, the Bitcoin standard for block size and maximum number of transactions per second present scalability concerns for large-scale and widely used blockchain applications.

Private and consortium led blockchains would address the privacy, security and scalability concerns. However, these blockchains would pose different challenges as they run the risk of not being vendor neutral and do not use open standards.

7. A Blockchain Model for Health Care

Any blockchain for health care would need to be public and would also need to include technological solutions for three key elements: scalability, access security and data privacy.

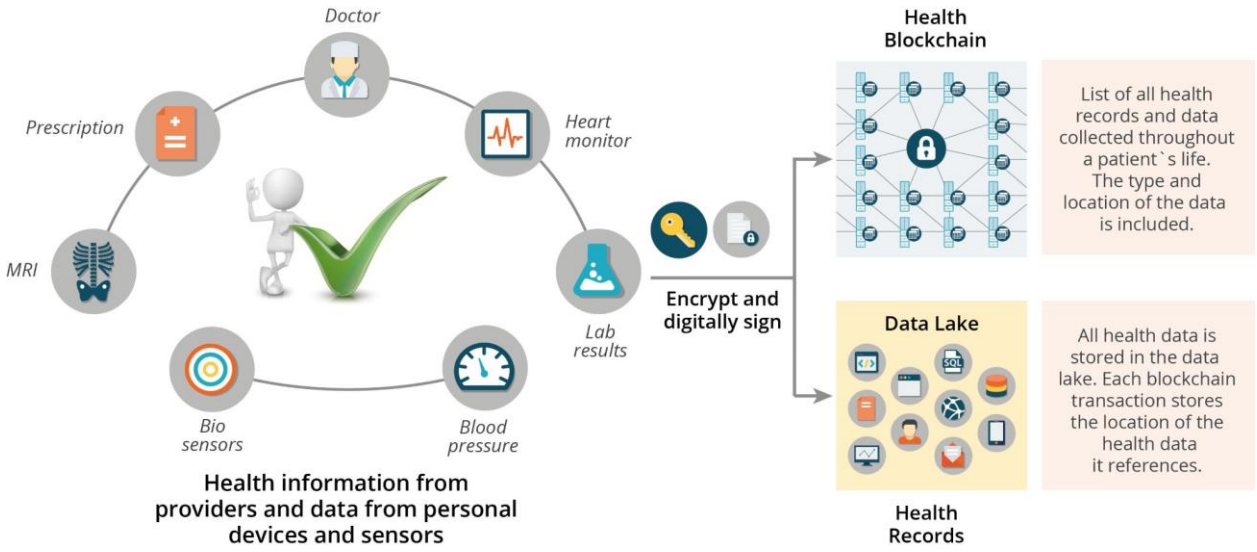
a. Scalability

A distributed blockchain that contains health records, documents or images would have data storage implications and data throughput limitations. If modeled after the Bitcoin blockchain, every member in the distributed network of the health care blockchain would have a copy of every health record for every individual in the world. and this would not be practical from a data storage perspective. Because health data is dynamic and expansive, replicating all heath records to every member in the network would be bandwidth intensive, wasteful on network resources and pose data throughput concerns. For health care to realize benefits from blockchain, the blockchain would need to function as an access-control manager for health records and data.

The information contained in our proposed health blockchain would be an index, a list of all the user's health records and health data. The index is similar to a card catalog in a library. The card catalog contains metadata about the book and a location where the book can be found. The health blockchain would work the same way. Transactions in the blocks would contain a user's unique identifier, an encrypted linked to the health record and a timestamp for when the transaction was created. To improve data access efficiency, the transaction would contain the type of data contained in the health record and any other metadata that would facilitate frequently used queries (the metadata could be added as tags). The health blockchain would contain a complete indexed history of all medical data, including formal medical records as well as health data from mobile applications and wearable sensors, and would follow an individual user throughout his life.

All medical data would be stored off blockchain in a data repository called a data lake. Data lakes are highly scalable and can store a wide variety of data, from images to documents to keyvalue stores. Data lakes would be valuable tools for health research and would be used for a variety of analysis including mining for factors that impact outcomes, determining optimal treatment options based on genetic markers and identifying elements that influence preventative medicine. Data lakes support interactive queries, text mining, text analytics and machine learning. All information stored in the data lake would be encrypted and digitally signed to ensure privacy and authenticity of the information.

When a health care provider creates a medical record (prescription, lab test, pathology result, MRI) a digital signature would be created to verify authenticity of the document or image. The health data would be encrypted and sent to the data lake for storage. Every time information is saved to the data lake a pointer to the health record is registered in the blockchain along with the user's unique identifier. The patient is notified that health data was added to his blockchain. In the same fashion a patient would be able to add health data with digital signatures and encryption from mobile applications and wearable sensors.

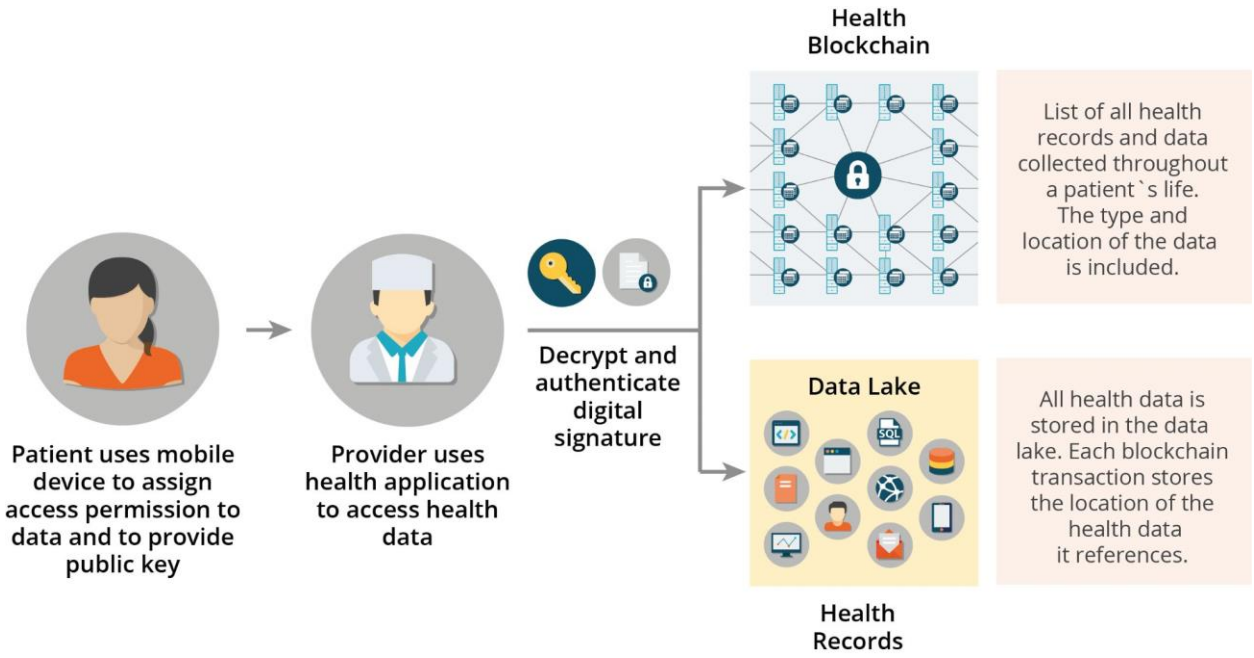


b. Access Security and Data Privacy

The user would have full access to his data and control over how his data would be shared. The user would assign a set of access permissions and designate who can query and write data to his blockchain. A mobile dashboard application would allow the user to see who has permission to access his blockchain. The user would also be able to view an audit log of who accessed his blockchain, including when and what data was accessed. The same dashboard would allow the user to give and revoke access permissions to any individual who has a unique identifier.

Access control permissions would be flexible and would handle more than “all-or-nothing” permissions. The user would setup specific, detailed transactions about who has access, the allotted time frame for access and the particular types of data that can be accessed. At any given time the user may alter the set of permissions. Access control policies would also be securely stored on a blockchain and only the user would be allowed to change them. This provides an environment of transparency and allows the user to make all decisions about what data is collected and how the data can be shared.

After a health care provider is granted access to a user’s health information, he queries the blockchain for the user’s data and utilizes the digital signature to authenticate the data. The health care provider could utilize a customized best-of-breed application to analyze the health data.



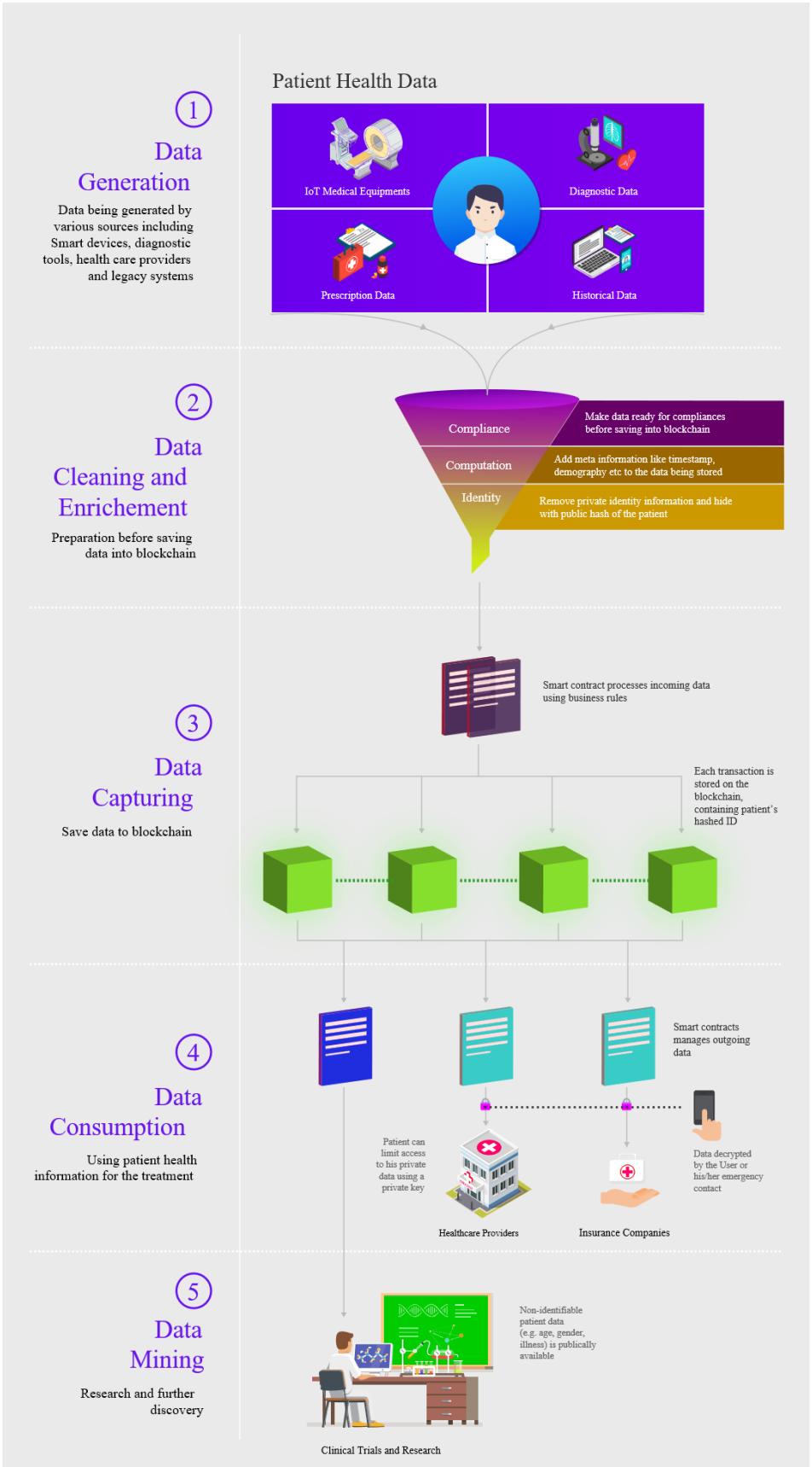
Identity authentication would follow the best practices established by financial institutions and regulators. Ideally, biometric identity systems would be utilized as they offer enhanced security over password and token (smartcard) based methods for identity authentication.

Given this model, the user has singular control over his data and the power to grant access to specific health care providers and/or health care entities for communication and collaboration in disease treatment and prevention. The decentralized nature of the blockchain combined with digitally signed transactions ensure that an adversary cannot pose as the user or corrupt the network as that would imply the adversary forged a digital signature or gained control over the majority of the network's resources. Similarly, an adversary would not be able to learn anything from the shared public ledger as only hashed pointers and encrypted information would be contained within the transactions.

8. Another Blockchain Model for Health Care

Healthcare blockchain solution for patient health record management can be divided into five primary modules:

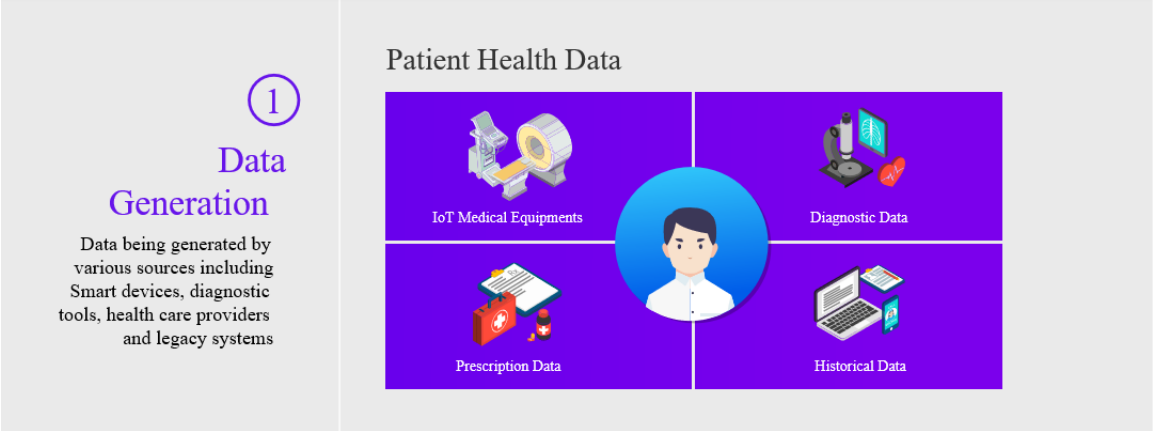
1. Data Generation
2. Data Enrichment
3. Storing health records on Healthcare blockchain
4. Data Consumption with Smart Contracts
5. Data mining and AI in Healthcare Blockchain


1
Data Generation
Data being generated by various sources including Smart devices, diagnostic tools, health care providers and legacy systems
Patient Health Data
IoT Medical Equipments
Diagnostic Data
Prescription Data
Historical Data
2
Data Cleaning and Enrichement
Preparation before saving data into blockchain
Compliance
Make data ready for compliances before saving into blockchain
Computation
Add meta information like timestamp, demography etc to the data being stored
Identity
Remove private identity information and hide with public hash of the patient
3
Data Capturing
Save data to blockchain
Smart contract processes incoming data using business rules
Each transaction is stored on the blockchain, containing patient's hashed ID
4
Data Consumption
Using patient health information for the treatment
Smart contracts manages outgoing data
Patient can limit access to his private data using a private key
Data decrypted by the User or his/her emergency contact
Healthcare Providers
Insurance Companies
5
Data Mining
Research and further discovery
Non-identifiable patient data (e.g. age, gender, illness) is publically available
Clinical Trials and Research

1. Data generation

To integrate blockchain in healthcare, first, we need to understand the scope of data and where and how it is being generated.

At every stage of medical treatment, whether it is a consultation, diagnosis, or surgery, healthcare companies generate sensitive and crucial medical data.



The medical data includes the doctor's prescriptions, X-rays, MRI scans, ultrasound reports, angiography, radiography, endoscopy, and so on. Healthcare data comes in various formats like text, paper, numeric, pictures, videos, digital, or multimedia. Though healthcare centers are adopting digital technologies, the patient's medical records are currently stored in the centralized servers. It creates the attack surface for hackers. Accenture's survey claims one in five employees working in the healthcare is willing to sell the sensitive medical data to the unauthorized parties. Electronic health records (EHR) contain exploitable information like name, address, place where you work, prescribed medicines, number of doctor visits and payment methods. A Medical record also contains sensitive protected health information like HIV diagnoses, cancer diagnoses, or psychological conditions. Recently, Grindr dating app has disclosed user's HIV status, sexuality, GPS position, and other personal details to third-parties. Sharing protected health information of patients without their consent can make them feel traumatized. Once the medical data of an individual is generated, data enrichment is done to make the data secure.

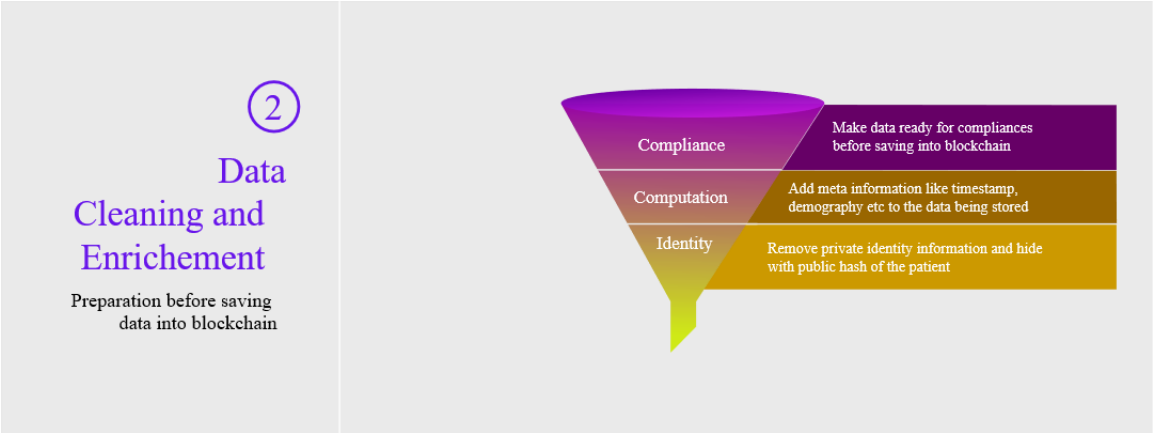
2. Data Enrichment- Before storing data to the blockchain

Data Enrichment is a process to add value to enhance the data quality.

Patient's health records need to be accurate, secure, understandable, time-stamped, and structured.

Storing unstructured data could lead to inconsistencies, delays in the treatment process, and inefficiencies.

It is essential to implement the following three steps to clean and secure the data before storing it on the blockchain.



a. Replace the patient's identity with the public hash key

A person's identity can be replaced by a hash, a unique numerical value. Replacing the user's identity with a hash would make it impossible for the attacker to decode the identity and protected health information (PHI). De-identifying the data will remove details including the patient's name, address, social security number and financial information. Data stored on blockchain is like your cryptocurrency such as bitcoin saved in the crypto wallet. Though the user's wallet can be identified with a public key, only a secret private key can help anyone read or understand the stored data. Any healthcare service provider would require patient consent or authorization to access PHI. If a patient denies sharing the medical data, no healthcare provider could get access to the records stored on the blockchain.

b. Make it compliance ready

Saving data on blockchain doesn't mean no-compliance. In fact, blockchain will make compliance enforcement more seamless and transparent. HIPAA (Health Insurance Portability and Accountability Act) Compliance ensures the protection of patient' data. Healthcare vendor that deals with patient's protected health information should follow HIPAA's security measures. HIPAA's privacy rule allows all the involved members to access and disclose only de-identified data. It is essential that the compliance check is maintained before the health records get saved on the blockchain.

c. Add Meta information and structure it for computation

Medical data categorized in multiple formats like administrative claim record, clinical registries, biometric data, patient-reported data, or medical imaging should be stored in a structured way. Organized data enables all healthcare providers to access data efficiently.

Add further information related to the timestamp, demographics, involved stakeholders, and eventually sign and provision the data to be stored on the blockchain.

The completion of the above steps adds value to the data to be stored on the blockchain.

We shall now discuss how health records can be stored on the blockchain.

3. Storing health records on healthcare blockchain

Blockchain can eliminate the risks associated with centralization of data by storing the digital health records across multiple nodes within the network.

Here's how Blockchain in healthcare could work:

To illustrate how could blockchain manage the medical records, we have further divided this module into four steps:

a. Health organizations store information on the blockchain:

Healthcare vendors can save health records with the patient's public key on the blockchain. Smart contracts get triggered to store the information provided by doctors, diagnostic centers, or health insurance companies on the blockchain.

b. Transactions are completed and identified uniquely:

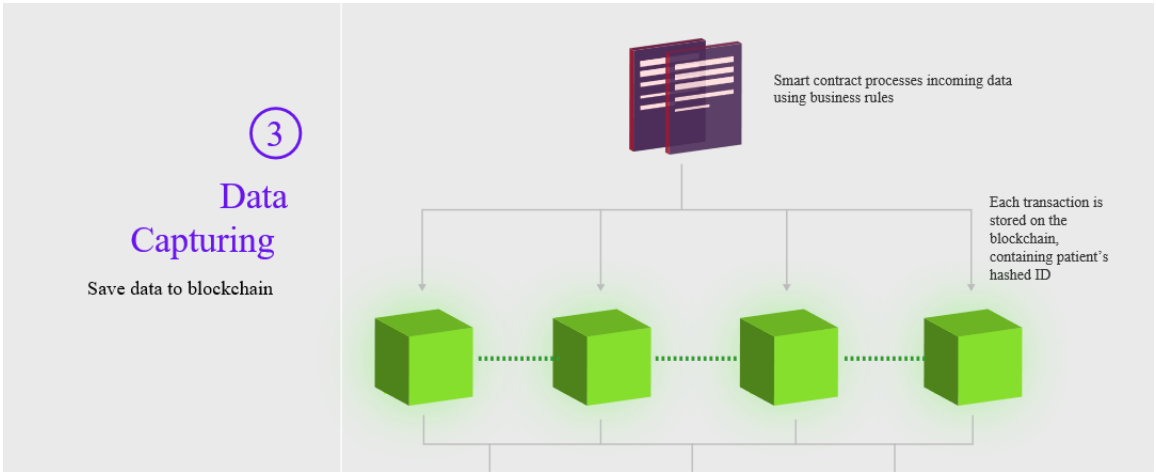
Transactions containing patient's health records are saved on the blockchain with their unique IDs and patient's public key. If a healthcare provider wants to access a patient's public non-identifiable data, transaction ID is matched, and the information is displayed.

c. Healthcare units can directly query the blockchain:

Unlike the traditional process, doctors or health insurance companies don't need to approach a patient for accessing their health records. Healthcare institutes can submit their queries via APIs and access the patient's non-identifiable information through smart contracts.

d. Patients can share their private key with health organizations:

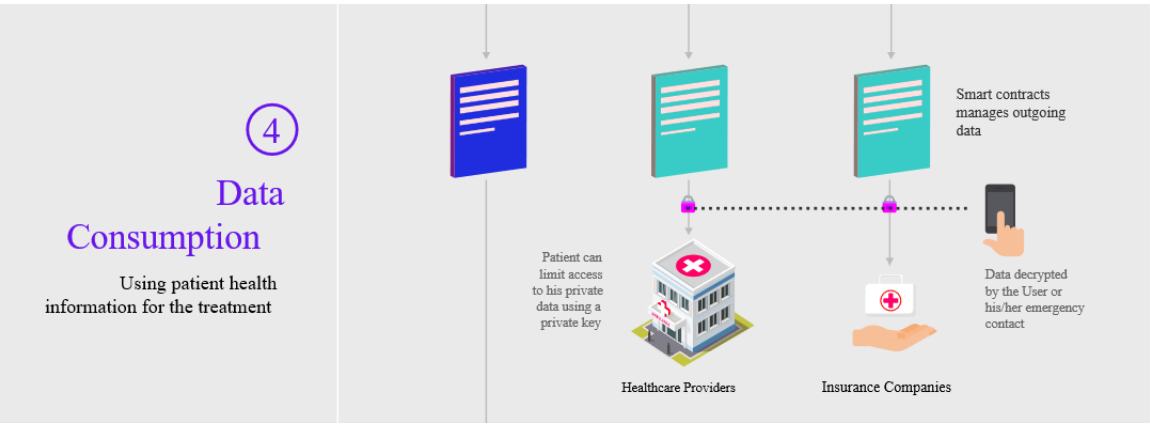
Blockchain healthcare solution can never reveal the patient's identifiable information until they provide their private key. Patients can share the private key with the health organizations if required. Data would always remain non-identifiable to healthcare providers without the secret key. It is similar to how cryptocurrencies are stored on the blockchain, where the owner with the private key can only access it.



A blockchain can either be a public or a private blockchain. Since a user identity will not be visible in this solution, a public blockchain could also be used.
Once the data is stored, it can be consumed by different healthcare blockchain vendors using smart contracts.

4. Data consumption with Smart contracts

Smart contracts ensure the enforcement of the business rules, compliance requirement, and the user's will before the data is shared or retrieved.
Stakeholders involved in the patient's treatment can consume the stored data with the patient's consent.
Let's understand how different healthcare providers could consume data using smart contracts:
a. When the data is saved on the blockchain, smart contracts are triggered.
b. Healthcare provider receives the patient's report with a hash that hides the identity.
c. Whenever a diagnostic lab or any other healthcare provider would request to access the patient's health records, smart contracts notify the patients.



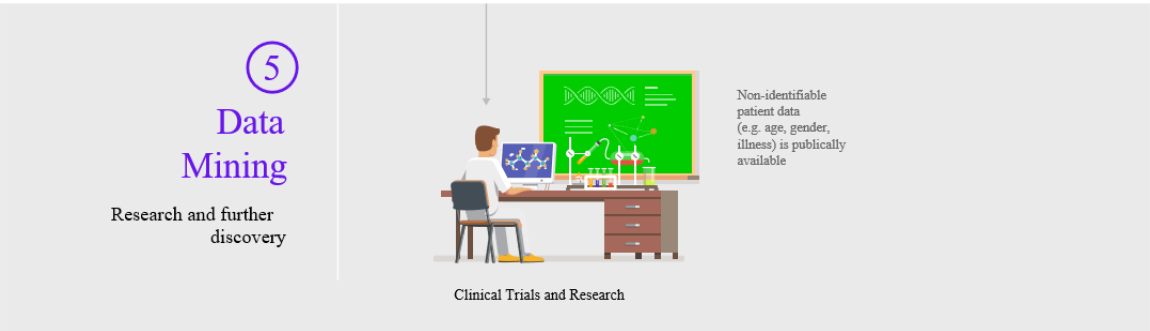
Smart contracts contain business logic about who gets what.
Insurance companies could only access the information related to billing and patient's diagnostic reports, but no other details such as doctor's notes or prescriptions.
Similarly, physicians in the healthcare centers could access relevant information such as the patient's historical health records, age, and diagnostic reports.
Patients would have ownership of the data, i.e., they can decide what information to be shared with which entity using smart contracts.
Smart contracts will ensure a transparent, conflict-free exchange of the information. In case, the user denies to exchange the information; no one could access the patient's health records.
Blockchain healthcare solution could also enable healthcare research companies to use health records for research purposes without affecting the patient's privacy. Read further to understand how.

5. Data Mining and AI in Healthcare Blockchain

Healthcare data nowadays is generated using different technologies like AI, IoT, or ML. The generated data can be used for multiple purposes, including disease prevention and cure, drug development, and clinical trials.

But the centralized approach for maintaining the data could hinder the patient's privacy. Blockchain could be leveraged to bring trust in the clinical trials and medical research process. As discussed above, the blockchain healthcare platform could use de-identification for hiding the patient's identity. So, medical research companies could utilize the non-identifiable records to carry out the research activities.

For example, if a research company wants to get the analytics for HIV disease, smart contracts would enable them to access details like HIV type, most-affected city or country, age group, and gender while hiding the personal information of patients.



Using Data Mining and AI along with the blockchain, research companies could discover the relevant data from the large data sets stored on the blockchain.

9. Benefits could Blockchain bring to the Healthcare Industry

In either ways mentioned in part 7 and 8, both approaches bring the same benefits as follows:

a. Simplified Approach to Data:
   Unlike a traditional way of managing information, healthcare records can be shared across multiple nodes using the healthcare blockchain.
   The need for storing data in multiple databases could be removed, hence, enabling the simplified approach to access the information.

b. System Interoperability:
   The inability to exchange healthcare records could lead to delays in treatment. But blockchain could alleviate this problem by decentralizing the data. Everyone within the healthcare network could access a transparent, yet immutable ledger while having the ownership of data.

c. Efficiency:
   Blockchain could turn the system highly efficient via real-time processing. It could remove the need for third-party companies, hence, eradicating the delays in accessing the data.

d. Control over the data:
   Anyone willing to access the health records would require the patient's public key. Patients could seamlessly control who should access what data.
   Since the data is saved in encrypted form, it remains unreadable to the hackers.

10. Health Care Advantages of Health Care Blockchain

Blockchain technology offers many advantages to medical researchers, health care providers, care givers and individuals. Creation of a single storage location for all health data, tracking personalized data in real-time and the security to set data access permissions at a granular level would serve research as well as personalized medicine.

Health researchers require broad and comprehensive data sets in order to advance the understanding of disease, accelerate biomedical discovery, fast track the development of drugs and design customized individual treatment plans based on patient genetics, lifecycle and environment. The shared data environment provided by Blockchain would deliver a broad diverse data set by including patients from different ethnic and socio-economic backgrounds and from various geographical environments. As blockchain collects health data across a patient's lifetime, it offers data ideal for longitudinal studies.

Blockchain data structures would work well for gathering data from wearable sensors and mobile applications and, thus, would contribute significant information on the risks versus benefits of treatments as well as patient reported outcomes. Furthermore, combining health data from mobile applications and wearable sensors with data from traditional EMR's and genomics will offer medical researchers increased capabilities to classify individuals into subpopulations that respond well to a specific treatment or who are more susceptible to a particular disease. Daily, personalized health data will likely engage a patient more in his own health care and improve patient compliance. Moreover, the ability for physicians to obtain more frequent data (i.e., daily blood pressures or blood sugar levels versus only when a patient appears for an appointment) would improve individualized care with specialized treatment plans based on outcomes/treatment efficacy.

Blockchain would ensure continuous availability and access to real-time data. Real-time access to data would improve clinical care coordination and improve clinical care in emergency medical situations. Real-time data would also allow researchers and public health resources to rapidly detect, isolate and drive change for environmental conditions that impact public health. For example, epidemics could be detected earlier and contained.

The real-time availability of mobile application and wearable sensor data from the blockchain would facilitate continuous, 24 hour-a-day monitoring of high risk patients and drive the innovation of “smart” applications that would notify care givers and health providers if a patient reached a critical threshold for action. Care teams could reach out to the patient and coordinate treatment options for early intervention.

A health care blockchain would likely promote the development of a new breed of “smart” applications for health providers that would mine the latest medical research and develop personalized treatment paths. The health provider and patient would have access to the same information and would be able to engage in a collaborative, educated discussion about the best-case treatment options based on research rather than intuition.

11. Conclusion

Blockchain opens up unique opportunities to create immutable and secure ledger, reduce complexities, and bring transparency. Considering the capabilities of the blockchain in healthcare industries, a decentralized platform could overcome the challenges faced by the healthcare sector. This is the reason that healthcare vendors are experimenting the potential of a healthcare data management solution.

Utilization of the proposed health blockchain described in this paper has the potential to engage millions of individuals, health care providers, health care entities and medical researchers to share vast amounts of genetic, diet, lifestyle, environmental and health data with guaranteed security and privacy protection. The acquisition, storage and sharing of this data would lay a scientific foundation for the advancement of medical research and precision medicine, help identify and develop new ways to treat and prevent disease and test whether or not mobile devices engage individuals more in their health care for improved health and disease prevention.

Bibliography

BitFury Group. (2016). *Digital Assets on Public Blockchains.* BitFury Group Limited.

Blockchain. (n.d.). Retrieved 7 2016, from Wikipedia: https://en.wikipedia.org/wiki/Blockchain_(database)

Fielder, S., & Light, J. (2015). *Distributed consensus ledgers.* Accenture, Accenture Payment Services. Accenture.

Form a Vital Link. (n.d.). Retrieved 8 2016, from pcori: http://www.pcori.org/

How does bitcoin work? (n.d.). Retrieved 7 2016, from Bitcoin: https://bitcoin.org/en/how-it-works

Kaye Scholer. (2016). *An Introduction to Bitcoin and Blockchain Technology.* www.kayescholer.com.

Lamport, L., Shostak, R., & Pease, M. (1982, 7). The Byzantine Generals Problem. (S. International, Ed.) *ACM Transaction on Programming Languages and Systems* .

Makary, M. A., & Daniel, M. (2016). *Medical error - the third leading cause of death.* BMJ. Monegro,

J. (n.d.). *The Blockchain Application Stack*. Retrieved 7 2016, from Joel Monegro Blog:

http://joel.mn/post/103546215249/the-blockchain-application-stack Nakamoto,

S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.*

(2015). Patient-Centered Health on the Blockchain with Chelsea Barabas.

Precision Medicine Initiative Cohort Program. (n.d.). *Precision Medicine Initiative Cohort Program*. Retrieved 7 2016, from

National Institutes of Health: https://www.nih.gov/precision-medicine-initiative-cohort-program Rodriguez,

J. (2015, 1 26). *Building an IOT Platform: Centralized vs. Decentralized Models*. Retrieved from

https://jrodthoughts.com/tag/enterprise-software/page/2/

Rogers, B. (2015, 11). *How the Blockchain and VR Can Change the Music Industry (Part 1)*. Retrieved 7 2016, from

https://medium.com/cuepoint/bc-a-fair-trade-music-format-virtual-reality-the-blockchain-76fc47699733#.q8lp7sxfl Rogers,

B. (2016, 2 24). *How the Blockchain Can Change the Music Industry (Part 2)*. Retrieved 7 2016, from

https://medium.com/cuepoint/how-the-blockchain-can-change-the-music-industry-part-2-c1fa3bdfa848#.gbiei2jc6

Schwartz, D., Youngs, N., & Britto, A. (2014). *The Ripple Protocol Consenus Algorithm.* Ripple Labs Inc. Ripple Labs Inc.

(2014). *Security and Compliance For Scale-Out Hadoop Data Lakes.* EMC.

Shead, M. (2009). Retrieved 2016, from Productivity501: http://www.productivity501.com/digital-signatures-encryption/4710/

The Office of the National Coordinator for Health Information Technology. (2015). *Connecting Health and Care for the Nation, A Shared Nationwide Interoperability Roadmap.*

Zyskind, G., & Nathan, O. (2015). *Enigma: Decentralized Computation Platform with Guaranteed Privacy.* MIT. MIT Media Lab.

Zyskind, G., Nathan, O., & Pentland, A. *Decentralizing Privacy: Using Blockchain to Protect Personal Data.* MIT. MIT Media Lab.

Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System . 2008 Oct; Available from: https://bitcoin.org/bitcoin.pdf

Buterin V. Visions, Part 1: The Value of Blockchain Technology [Internet]. Ethereum Blog. 2015 [cited 2017 Jul 13]. Available from: https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/

Brodersen C, Kalis B, Leong C, Mitchell E, Truscott A. Blockchain: Securing a New Health Interoperability Experience. 2016 Aug; Available from: https://www.healthit.gov/sites/default/files/2-49-accenture_onc_blockchain_challenge_response_august8_final.pdf

Mandl KD, Kohane IS. Escaping the EHR trap--the future of health IT. N Engl J Med. 2012 Jun 14;366(24):2240–2.

Krawiec RJ, Housman D, White M, Filipova M, Quarre F, Barr D, et al. Blockchain: Opportunities for Health Care. 2016 Aug; Available from: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchainopportunities-for-health-care.pdf