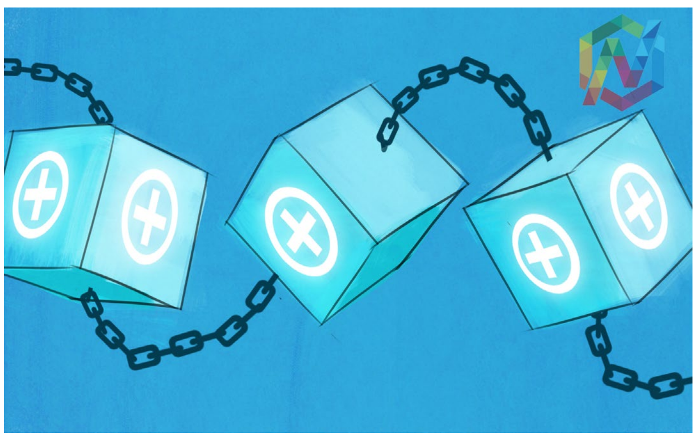
CIS 9797

Blockchain Final Project

A New Model for Health Information Exchanges



By

Shobhit Ratan

Aliona Ravlov

December 16, 2018

Table of Contents

Introduction

The existing public health information technology systems such as eligibility, enrollment and electronic health records have documented issues with interoperability and are slow to adapt to changing program and technology demands. A decentralized benefits administration system can provide greater efficiency to enrollment, eligibility, claims payment and adjudication processes thus driving efficiency and reducing systemic fraud (David Randall).

Figure1:Production Healthcare Systems are Often Unable to Interoperate, and Access to Data Records is Disabled by Disparate and Siloed Systems (Peng Zhang)

Figure 1 depicts barriers to achieving healthcare system interoperability, including incompatible software and the lack of access to data outside a healthcare environment (such as a firewall protected clinic database or a patient-collected mobile health data). A promising solution to these problems involves the application of Blockchain technology, which provides "trustless" transactions via decentralization with pseudo-anonymity. (Peng Zhang)

Health Information Exchange (HIE) is a public blockchain based application that would advance Interoperability within the healthcare industry. Key desired objectives are : scalability, access security and data privacy (Linn LA). A blockchain powered health information exchange could unlock the true value of interoperability. Blockchain-based systems provide data integrity, decentralization and disintermediation of trust, and reduced transaction costs. 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. Prominent areas of Healthcare ecosystem that can benefit from blockchain technology are as follows :

- Clinical Administrative & Backend Scheduling, patient transfers, billing compliance
- Medical Devices & Diagnostics Monitoring, detection equipment
- Doctor & Healthcare Service Search Services to search for doctors, healthcare plans,and specialized healthcare
- Doctor Network & Resources Collaboration platform across hospitals and social networks that identify and share bestpractices

- Electronic Health/Medical Records Platforms for electronic medical charts, schedules, prescription tracking and referral letters

Phases of adding a block to the healthcare blockchain are shown in Figure 2 below:

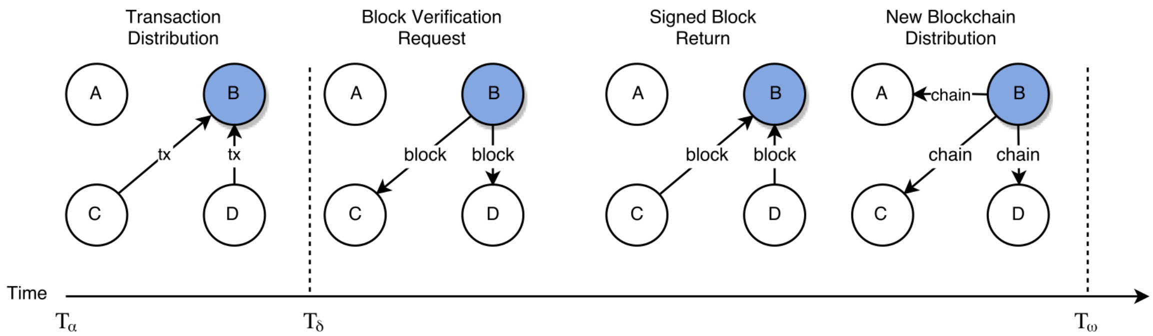


Figure 2: Phases of adding a block to the healthcare blockchain (Peterson)

Blockchain has potential to improve healthcare in a number of innovative ways. Some of those examples include a Master Patient Identifier (MPI), autonomous automatic adjudication and interoperability. In addition to offering interoperability, blockchain transactions would also have the advantage of being cryptographically and irrevocable thus ensuring privacy across parties. (David Randall) HIE pain points and corresponding blockchain opportunities are shown in Figure 3.

HIE pain points	Blockchain opportunities
Establishing a trust network depends on the HIE as an intermediary to establish point-to-point sharing and "book-keeping" of what data was exchanged.	**Disintermediation of trust** likely would not require an HIE operator because all participants would have access to the distributed ledger to maintain a secure exchange without complex brokered trust.
Cost per transaction, given low transaction volumes, reduces the business case for central systems or new edge networks for participating groups.	**Reduced transaction costs** due to disintermediation, as well as near-real time processing, would make the system more efficient.
Master Patient Index (MPI) challenges arise from the need to synchronize multiple patient identifiers between systems while securing patient privacy.	**Distributed framework for patient digital identities**, which uses private and public identifiers secured through cryptography, creates a singular, more secure method of protecting patient identity.
Varying data standards reduce interoperability because records are not compatible between systems.	**Shared data** enables near real-time updates across the network to all parties.
Limited access to population health data, as HIE is one of the few sources of integrated records.	**Distributed, secure access** to patient longitudinal health data across the distributed ledger.
Inconsistent rules and permissions inhibit the right health organization from accessing the right patient data at the right time.	**Smart contracts** create a consistent, rule-based method for accessing patient data that can be permissioned to selected health organizations.

Figure 3: HIE Pain Points with corresponding Blockchain opportunities (RJ Krawiec)

Blockchain technology offers many advantages for health care IT. It is based on open source software, commodity hardware, and open API's. These components facilitate faster and easier interoperability between systems and can efficiently scale to handle larger volumes of data and more blockchain users. The architecture has built-in fault tolerance and disaster recovery, and the data encryption and cryptography technologies are widely used and accepted as industry standards. (RJ Krawiec). Figure 4 & 5 represent an *illustrative framework for the healthcare blockchain ecosystem* and *blockchain's decentralised P2P architecture* respectively.

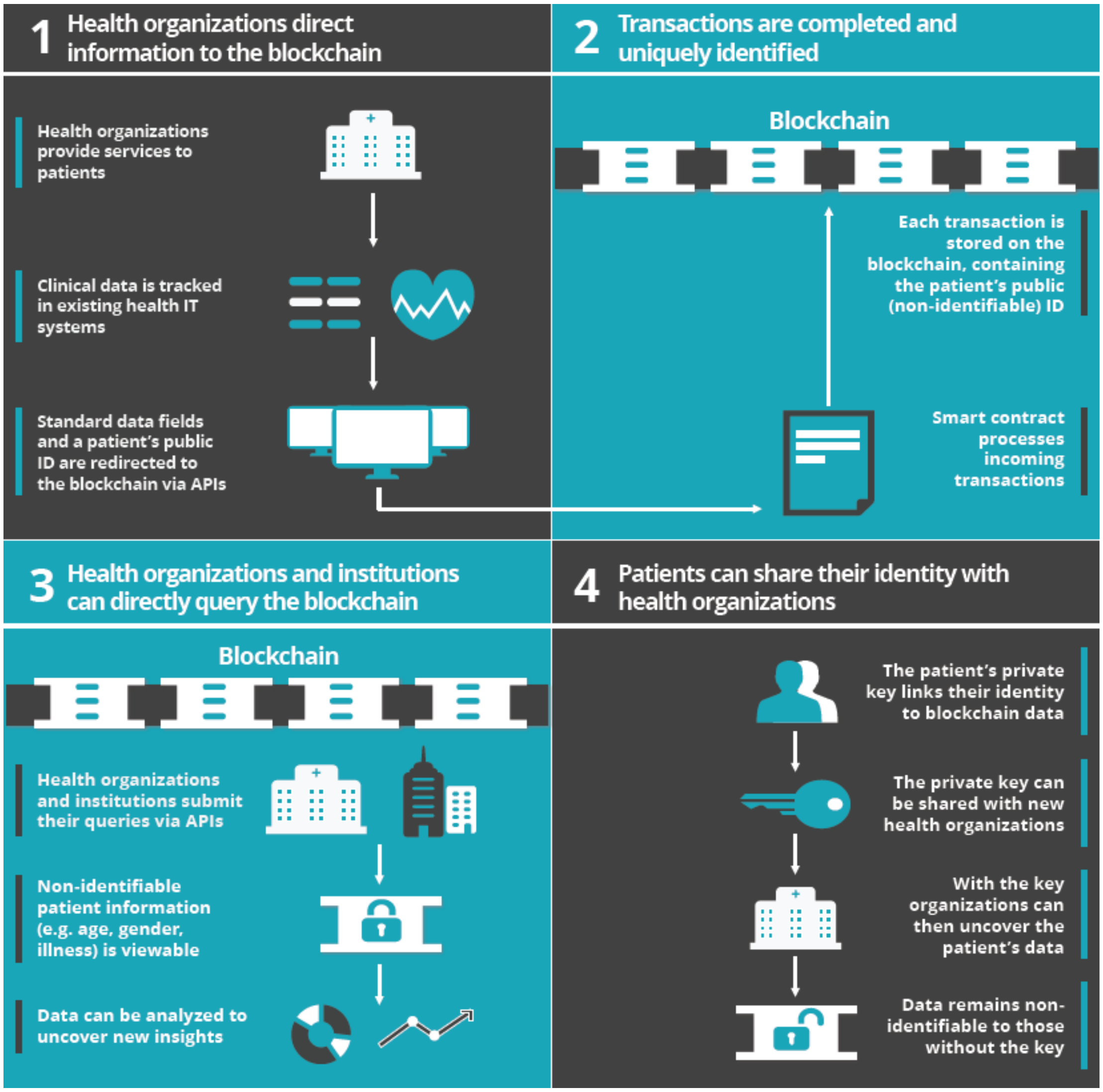


Figure 4: Illustrative Framework of Healthcare Blockchain Ecosystem (RJ Krawiec)

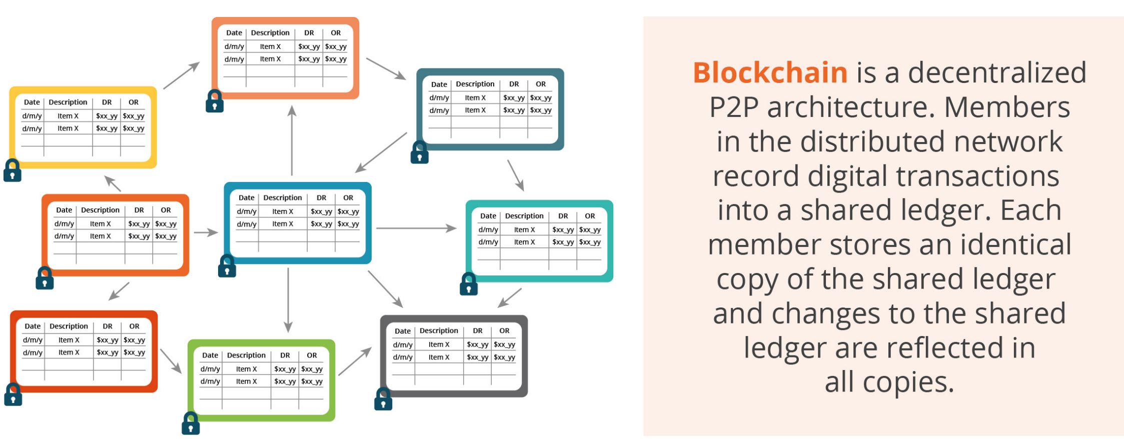


Figure 5: Blockchain – A decentralized P2P architecture (Linn LA)

Blocks in our health blockchain would contain a user's unique identifier, an encrypted link 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 (Linn LA).

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 hash 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 (Linn LA).

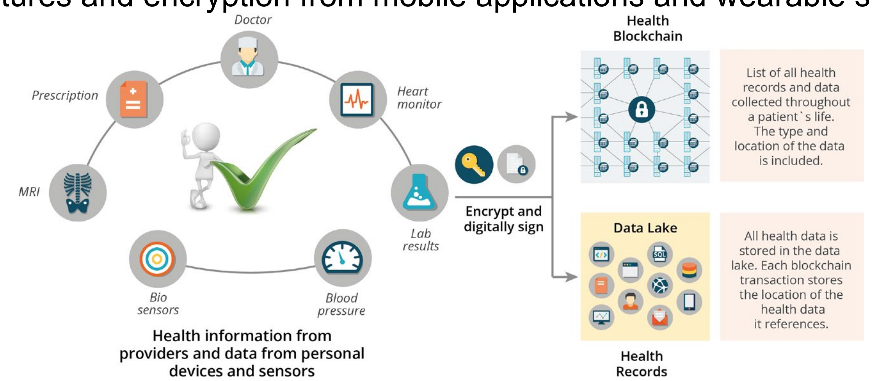


Figure 6 : Patient Adding Health Data using Digital Signatures and Encryption

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. 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 (Linn LA).

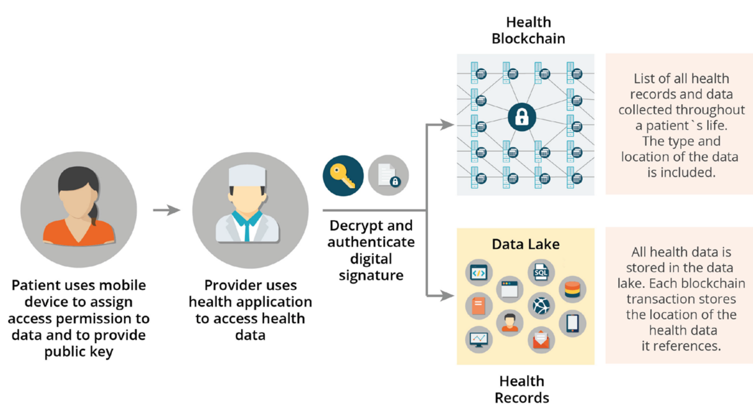


Figure 7 : Health Care Provider using Digital Signatures to authenticate the data

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 51% 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.

Answer to Project Questions with relevance to Health Information Exchange Blockchain Application

1. Why is a blockchain used?

A blockchain based system will offer a distributed framework to amplify and support the integration of health-care information across a range of users and stakeholders. It addresses existing issues and enables a system that is more efficient, disintermediated, and secure. Further, blockchain provides a tamper-proof ledger based on hash pointers and it is thus infeasible for an adversary to modify or update the transaction ledger.

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. 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. A health care blockchain would expand the acquisition of health data to include data from populations of people who are currently under-served by the medical community or who do not typically participate in research (Linn LA).

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. For example, epidemics could be detected earlier and contained (Linn LA).

2. Are any other data structures used and why?

HIE Blockchain is a shared peer to peer network built from linked transaction blocks and stored in a digital ledger. It is using a Merkle Tree data structure. The transactions are hashed and stored in the block. Next, the hashes of two transactions are taken and hashed further to generate another hash. This process at the end provides a single hash from all transactions stored within a block. This hash is called transaction Merkle Root hash and is stored in Block's header. Therefore, any change made in any of the transactions will result in change in hash and therefore change in root transaction hash. This helps making transactions immutable. Further, it also uses Data Lakes data structure. Blockchain data structures combined with data lakes can support a wide variety of health data sources including data from patients' mobile applications, wearable sensors, EMR's, documents and images. The data structures are flexible, extendable and would be able to accommodate the unforeseen data that will be available in the future. Another advantage of blockchains distributed architecture is built-in fault tolerance and disaster recovery. Data is distributed across many servers in many different locations. There is no single point of failure and it is unlikely a disaster would impact all locations at the same time (Linn LA).

3. Which hashing function is used and why?

The blockchain system will use cryptographic hash function SHA256. Using SHA256 hashing algorithm and function with any length will always generate a 256-bit output data. This hashing function is especially useful as large amount of data can be stored as a 256-bit output. HIE blockchain based system hashes all the transaction data, hashes multiple transaction hashes to generate single root transaction hash and the blocks in this system are also represented as a hash. An important property of hashing is that it is mathematically not feasible to identify two different input strings that will output the same hash. In other words, it is not possible to computationally and mathematically find the input from the hash itself. The Blockchain creates a hash for each HIE block, together with a patient ID. Using an API, covered entities can receive the necessary information without revealing a patient's identity. In the same way, a patient can decide whom to provide with access and whether this access will be either full or partial. Furthermore, a patient can set specific third parties that would have to give their permission for sharing the HIE, if the patient is not sure in what he or she is doing.

4. Are digital signatures used? If so, which scheme is used and why?

The participants connected to the blockchain network have a secret private key and public key that act as an identifier. The pair is cryptographically linked such that the identification is possible through the private key. In this scheme, one has to possess the private key in order to unlock participant's identity and uncover what information on the blockchain is relevant to participant's profile. This private/public scheme key encryption scheme creates identity permission layers that allows patients to share distinct identity attributes with given health care organizations. We plan on using ECDSA digital signature scheme as it makes it infeasible for an adversary to forge a signature provided there is good randomness. This will be specially required in a health information exchange system as we don't want an adversary to forge our signatures and compromise sensitive patient, hospital and other service providers data.

5. What goes in each block?

Much like the Bitcoin approach, the block is a Merkle Tree-based structure. The leaf nodes of this tree represent patient record transactions, and describe the addition of a resource to the official patient record. Transactions, however, do not include the actual record document. Instead, they reference Fast Healthcare Interoperability Resources (FHIR) via Uniform Resource Locators (URLs). This allows institutions to retain operational control of their data, but more importantly, keeps sensitive patient data out of the blockchain.

➢ *Each block contains*:

- *Hash*: The SHA256 hash of the resource payload. Although the actual resource itself is not entered into the blockchain, its content can be verified using the transaction hash upon retrieval.
- *Contributor Signature*: The digital signature of the originating node.
- *FHIR URL*: A reference to the actual FHIR resource location.
- *FHIR Profile*: The URL of the FHIR Profile to which this resource conforms.
- *Secure Index*: An encrypted index allowing for data discovery without leaking information about the record.

➢ *The hashes of all transactions in a block contribute to the hash of the Merkle Root, or Block Header. The Block Header contains the following metadata used to validate the new block:*

- *Hash*: The SHA256 hash of the block. Assume the Merkle Root has two children c_0 and c_1, with a previous block b_{n-1}. Let the hash of b_n equal the hash of the hashed concatenation of the of the b_{n-1}, c_0, and c_1 hashes.
- *Previous Block Hash*: The hash of the previous block, for validation purposes.
- *Contributor Signatures*: For each node that contributed to the block, a digital signature is required. This is to ensure that the block remains valid after it was assembled by the miner.
- *Miner Elections*: Each node that contributed to the block is required to provide a random number encrypted with the node's private key. This will be used to seed the election of the next miner.

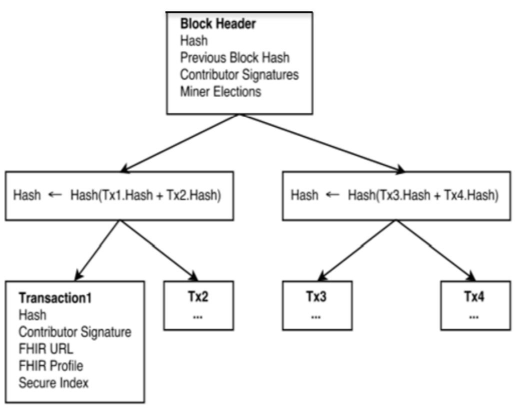


Figure 8 : Blockchain Structure *(Peterson)*

6. How are blocks added to the chain?

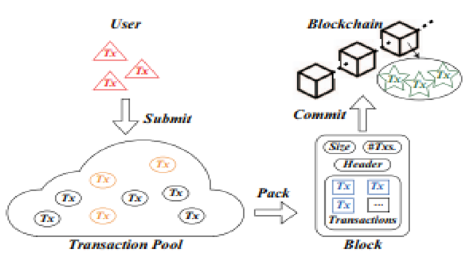


Figure 9: Procedure for Commiting Transactions *(Shan Jiang)*

As shown in Figure 9, a block is added to the blockchain at regular intervals of time, similar to that in Bitcoin. For Bitcoin, this interval is determined by the difficulty of the Proof of Work function. For this network, the difficulty is specified at a constant interval of time for creating a block, or a block period. Within this block period, the network undergoes four phases of activity. During *Transaction Distribution* phase (Phase 1) starting at time T_α, the transactions are sent to the coordinating, or miner node. This phase continues until T_δ, when the miner node may stop accepting new transactions for the block. The miner then assembles the new block and sends it to the nodes for review in the *Block Verification Request* phase (Phase 2). This allows all nodes that have contributed at least one transaction to digitally sign the block, indicating that they endorse its correctness. The block is then returned to the miner in the *Signed Block Return* phase (Phase 3). The miner node then adds the block to its local blockchain, and finally distributes the new blockchain in the *New Blockchain Distribution Phase* (Phase 4) (Shan Jiang).

7. How is the "health" of your blockchain maintained?

HIE Blockchain network consists of multiple nodes belonging to miners and some nodes that do not mine but helps in execution of smart contracts and transactions. Each node is connected to other node on the network. These nodes use peer-to-peer protocol to talk to each other. Each miner maintains an instance of ledger. Ledger contains all blocks in the chain. With multiple miners it is quite possible that each miner's ledger instance might have different blocks than other. The miners synchronize their blocks on an on-going basis to ensure that every miner's ledger instance is same as the others.

8. Describe any consensus mechanism?

The goal of HIE network is to avoid a Proof of Work model, where network computational power is expended without providing something intrinsically valuable. Rather, through the means of Proof of Interoperability model, this application aims to arrive at network consensus by forcing nodes to provide proof that the data in a transaction references can be meaningfully interpreted, while at the same time requiring nodes to verify these validity proofs.

Proof of Interoperability is an alternative method that is designed to leverage the effort required to reach network consensus to do something intrinsically valuable: to verify that incoming messages are interoperable with regard to a known set of structural and semantic constraints. For the case of this application, the mechanism for designating these interoperability constraints is the *FHIR Profile*. Profiles in FHIR are a mechanism to further constrain a FHIR resource by introducing a model for computable conformance statements. This conformance is both structural and semantic, allowing not only structural constraints on attributes such as cardinality and type, but semantic constraints using value sets. Given a transaction, the specified FHIR Profile is compared to the known set of allowable Profiles. If the Profile is recognized, conformance to the Profile is checked via the Check Profile Conformance function. This operation will use the FHIR URL to make a validate1 request to the FHIR server. The result of this request is a FHIR OperationOutcome response, which can then be inspected for conformance by the Conforms function. Proof of Interoperability does require the network to reach consensus on the set of allowed FHIR Profiles, including the content of the attendant value sets. This consensus cannot, however, be reached programmatically. Network agreement is most likely a human-based process, where network participants negotiate and collaborate with the help of both terminology specialists and clinicians (Peterson).

9. Describe how your network maintains security and any possible attacks which can be made?

Each HIE blockchain network participant has a secret private key and a public key that acts as a visible identifier. This pair of keys is cryptographically linked so that identification is possible only in one direction by using the private key that unlocks a participant's profile.Since there are identity permission layers, patients can limit data access and share relevant parts of their personal information with particular providers on base on need basis.

In this system, potential hacking of a particular patient's private key to access its identifiable data and alter this data is limited since the hacker would need to individually hack every single user to obtain unique private keys to access identifiable information of value. Additionally, all healthcare organizations connected to the blockchain can maintain their own updated copy of health care ledger and even if a historical block were to be adjusted it would require 51% of network participants to approve the change, as every single copy of the blockchain will need to be updated to reflect this change. This feature improves security and helps to limit the risk of a malicious activity since all changes are broadcasted within the network and distributed ledgers provide multiple copies which provide safeguard from harmful hacks. In order to prevent a 51% attack we will use virtual mining to mine the blocks.

HIE Blockchain also helps with frictionless connectivity since it's supported by smart contracts and consistent authorization to access health data. Smart contracts play a role of a gateway to store standardized information, which all network participants can immediately access, due to API-oriented architecture. This architecture allows for seamless integration with each organization's existing systems, so providers can focus on their internal systems (Shiklo).

10. Describe how your blockchain can "scale"?

Over the few years, one of the criticisms for Bitcoin and Ethereum has been its maximum size of blocks. Bitcoin blocks have a maximum size of 1 MB and only 7 transactions are processed per second whereas Paypal can process up to 100 transactions / second. Similarly, Ethereum can only process 15 transactions / second. Our aim is to build an application which increases the maximum size of blocks to 4 MB and can process 30 transactions / second. Larger block size and faster transaction speed will result in increased number of users, thus providing scale to HIE Blockchain. Even though, critics may argue that increasing the size of the blockchain may increase expenses in operating the full nodes and may lead to decrease in decentralization. However, speed and efficiency to process transactions faster are important considerations for consumers and slow transaction processing speed is one of the reasons for decline in users. With our strategy, we may see a temporary increase in expenses however it will be offset by the increase in number of users.

11. Describe if or how any component of your application could be valued. (i.e. the economics of your application).

Business Value/Incentives. We seek to help patients protect their privacy by providing a secure HIE application, which can provide patients and providers the desired medical information exchange.Both the patient and the provider are positioned to benefit from a robust data exchange platform. Viewed from both perspectives, one may see that the quantifiable benefits gained by providers and organizations are paralleled by greater convenience and better care outcomes for the patient.

Patient Perspective:

- Patients no longer need to coordinate the tedious and frustrating task of gathering records from various providers to send to their specialist. Instead, they would provide the specialist access to the blockchain, enabling them access to the data as they see fit.
- Patients retain control of their data without having to be data stewards, i.e they no longer have to spend time and energy keeping their data managed and up to date. They also no longer need to manually reconcile the data when they visit multiple providers, which can be a non-trivial task.
- Ultimately, better and more available data leads to better care for the patient.

Provider and Organization Perspective:

- The true collaborative nature of creating and sharing data would eliminate many of the challenges of existing Health Information Exchange approaches.
- Healthcare organizations do not have to fight for a data-driven competitive advantage, because they all have access to the same information. This approach will enable organizations to collaborate on care coordination and outcomes-based care.
- Through existing trust/contracts with patients and partner hospitals/organizations, nodes can broadcast alerts or potential threats.
- Data can be shared for research activities including clinical trials, enabling larger and more diverse patient populations.

12. Describe how your application can be updated?

Our application can only be updated through soft forking and checkpointing as we don't want malicious users to have the ability to fork the chain and subvert patient information. Without checkpointing, malicious miners can flood the network with valid, fake blocks that have mathematically valid but fake solutions that will undermine our HIE application. We also plan to implement a proposal like "Slasher" which allows punishment of miners who attempt to fork the chain. Slasher requires users to sign the current block with their private key corresponding to the transactions making up the miner's stake. This mechanism can allow users to catch the proof of misbehavior. Users can however add new signature schemes, extra metadata and new scripting features. Advantage of soft fork is that a branch is still considered to be valid and old miners will still build in top of the new branch so users are not forced to upgrade to the new features.

13. If applicable, how do users interact with your application?

The system architecture of Blockchain for health information exchanges is presented in the figure below. This blockchain system is envisioned for storing and sharing healthcare data between medical institutions and individuals. There are mainly three components in this blockchain architecture. The first component is the Blockchain network. The Blockchain network is responsible for storing and sharing the collected healthcare data. Anyone who is willing to contribute to this platform can join the network. The medical institutions, hospitals and clinics, act as the second component. When there are new patients in a hospital, their diagnostic records will be submitted to the Blockchain network and shared with other hospitals and clinics. The third component consists of all the individuals who are willing to store and share their daily healthcare data. In a smart home, numerous healthcare data are generated by the IoT devices, e.g., smart watch, smart thermometer, and smart sphygmomanometer. These devices can automatically submit the generated data to the Blockchain network (Shan Jiang).

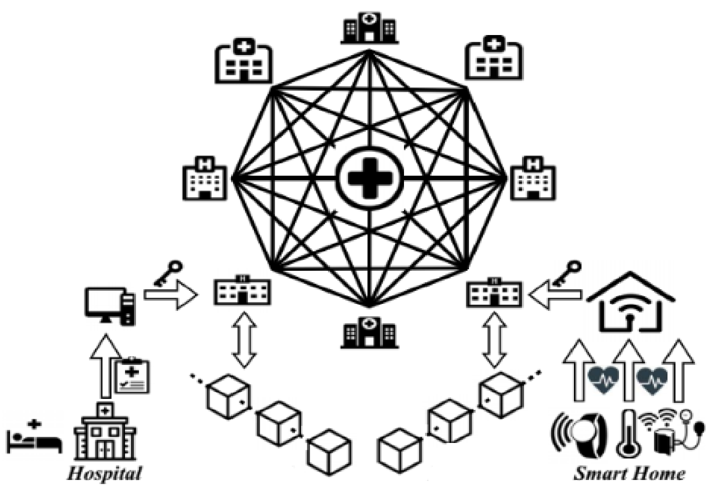


Figure 10: User-Interaction Overview *(Shan Jiang)*

Among the three components, there are two parties, medical institutions and individuals, who are submitting and sharing healthcare data in Blockchain. The reason why they are separated is that there are different requirements to share their data. For medical institutions, what they submit are medical diagnostic report, medical examination report. These data are incredibly privacy-sensitive. Moreover, there is a high demand to authenticate these data. For example, if a patient receives some treatment in a medical hospital and the medical diagnostic report is published with the signatures from both the hospital and the patient, neither the hospital nor the patient can deny the treatment. When it comes to the data generated by the individuals, the primary concern is the quantity. The amount of healthcare data generated by each person is remarkable. The key requirements to publish and share individuals' data are high throughput and substantial fairness.

14. Discuss any political/regulatory issues associated with your application.

Health Insurance Portability and Accountability Act (HIPAA) privacy rule established national standards to protect individuals medical records. The Rule limits the use and disclosure of patients information without the specific authorization provided by the patient. Blockchain implementations that allow for selective disclosure of private information (e.g. such as Zcash) and rely on zero knowledge cryptography to provide verification of transactions with a high degree of privacy over the underlying data will be provided by the HIE blockchain application (William J. Gordon).

15. Describe, if applicable, the role of any exchange regarding your application.

We are building an health information exchange for patients and suppliers. We want to build a network where suppliers can exchange altcoins/bitcoins/fiat-currency for patient information. In today's economy, knowledge is power where we want to be able to provide health information to our patients and suppliers as quickly as possible in order to take the right course of action. We don't want to intermediaries to be involved on our network as there might be a breach of trust between the intermediaries and the patients.

16. Within reason, tell me anything else of interest about your application.

Future directions:

Aggregate Blockchains. Heath Information Exchanges, tend to be groupings of institutions / regional providers. We conceptualized nodes in a data sharing network as individual institutions or providers. If we envision a node not as a single institution, but as an entire blockchain-based data sharing network then, we can not only imagine cross-institutional sharing, but also cross-network sharing. This notion of aggregation, or nested blockchains, may be an approach to extend the reach of collaborations and share beyond local networks (Peterson).

Fusion of AI and Blockchain Technologies in Healthcare. With the rapid improvement in computational power and machine learning algorithms, blockchain technology can help facilitate a mechanism to compensate an Artificial Intelligence (AI) service provider for the development and execution of novel machine learning algorithms. For example, developing machine learning algorithms that can look at a radiology image or CT scan and make diagnosis predictions are time consuming to develop, but once developed are easy to execute. By leveraging blockchain technology, one can envision a world in which a service provider publishes FHIR Diagnostic Reports of radiology images to the blockchain. Hospital can partner with an AI service provider, that specializes in developing novel machine learning algorithms to read the images and publish the AI diagnostic output back to the blockchain. The radiologist at the hospital could then use this result as an independent reference to compare his or her own diagnosis. The AI providers get compensated when their diagnosis matches that of the radiologist, so there is an incentive for the AI providers to refine and keep improving the accuracy of their algorithms for correct reporting/diagnosis. The blockchain also provides an irrefutable trail of what the AI provider diagnosed and the final official diagnosis (Peterson).

Conclusion

Blockchain technology in health care, based on open standards, addresses interoperability challenges, provides a shared distributed view of health data and has huge potential to achieve widespread acceptance and deployment. Health Information Exchange (HIE) blockchain application can 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 (Linn LA).

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. The real-time availability of mobile application and wearable sensor data from the blockchain would facilitate round the clock monitoring of high risk patients. The shared data environment provided by Blockchain makes it easier to engage “hard-to-reach” populations and develop results more representative of the general public (Linn LA).

A blockchain solution could address the HIPAA Privacy Rule by separating and encrypting identity, Personally Identifiable Information(PII), and Protected Health Information (PHI). A blockchain-enabled, trusted exchange of health information can provide longitudinal views of patients’ health, generate new insights about population health, and support the move toward value-based care. With greater transparency, trust, and access to data, Dept of Health and Human Services (HHS) can then also garner insights for better safety, effectiveness, quality, and security of foods, drugs, vaccines, and medical devices. In the long term, a nationwide blockchain network may improve efficiencies and support to providers and better health outcomes for patients (RJ Krawiec).

Works Cited

David Randall, Pradeep Goel and Ramzi Abujamra. *Blockchain Applications and Use Cases in Health Information Technology*. Washington, DC, USA: American Research and Policy Institute, n.d.

Linn LA, Koo MB. *Blockchain for health data and its potential use in health IT and health care related research*. Gaithersburg: ONC/NIST Use of Blockchain for Healthcare and Research Workshop, 2016.

Peng Zhang, Douglas C. Schmidt, Jules White and Gunther Lenz. *Book Chapter Proposal for Chapter 3: Blockchain Technology Use Cases in Healthcare*. Nashville, Palo Alto: Vanderbilt University, Varian Medical Systems, n.d.

Peterson, Kevin, Rammohan Deeduvanu, Pradip Kanjamala, Kelly Boles, and Mayo Clinic. "“A Blockchain-Based Approach to Health Information Exchange Networks”." 2016.

RJ Krawiec, Dan Housman, Mark White, Mariya Filipova, Florian Quarre, Dan. "Blockchain: Opportunities for Health Care." 2016.

Shan Jiang, Jiannong Cao, Hanqing Wu, Yanni Yang, Mingyu Ma, Jianfei He. *BlocHIE: a BLOCkchain-based platform for Healthcare Information Exchange*. Hong Kong: The Hong Kong Polytechnic University, Huawei Technology Ltd. , n.d.

Shiklo, Boris. "How Blockchain Can Improve The Health Information Exchange." 27 June 2017. *Forbes.*

William J. Gordon, Christian Catalini. "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability." *Computational and Structural Biotechnology Journal* (April, 13, 2018): 224-229.