A Blockchain-Based Approach to Health Information Exchange Networks

Kevin Peterson, Rammohan Deeduvanu, Pradip Kanjamala, and Kelly Boles

Mayo Clinic

Abstract

Sharing healthcare data between institutions is challenging. Heterogeneous data structures may preclude compatibility, while disparate use of healthcare terminology limits data comprehension. Even if structure and semantics could be agreed upon, both security and data consistency concerns abound. Centralized data stores and authority providers are attractive targets for cyber attack, and establishing a consistent view of the patient record across a data sharing network is problematic. In this work we present a Blockchain-based approach to sharing patient data. This approach trades a single centralized source of trust in favor of network consensus, and predicates consensus on proof of structural and semantic interoperability.

1 Problem Statement

Cross-institutional sharing of healthcare data is a complex undertaking with the potential to significantly increase research and clinical effectiveness[1]. First and foremost, institutions often are reluctant to share data because of privacy concerns[2], and may fear that sending information will give others a competitive advantage[3]. Next, even if privacy concerns could be addressed, there is no broad consensus around the specific technical infrastructure needed to support such a task[4]. Finally, healthcare data itself is complex, and sending information across institutional boundaries requires a shared understanding of both data structures and meaning. Even assuming data can be shared efficiently and securely, these interoperability issues left unchecked will limit the utility of the data. Despite evidence that the value of healthcare data exchange is large[5], these issues, described below, remain significant barriers.

1.1 Security

Failing to secure the patient record has financial and legal consequences, as well as the potential to impact patient care. Securing the electronic medical record is a challenging task[6], and the ramifications of a breach are a strong disincentive to sharing data. For this work, we focus on both *privacy* and *anonymity* and how they apply to data sharing.

Data privacy involves ensuring only authorized parties may access the medical record. This impacts any healthcare system, as patient privacy is not only an ethical responsibility, but a legal mandate[7]. Patient data is also an asset to the institution, and unauthorized access could compromise competitive advantages or reveal proprietary practices.

Data anonymity may also be used to secure the record. In this way, identifiable information is left out, and only summary/partial data is shared. This can be acceptable, but is challenging, as it requires a large number of attributes with potential resource or patient care value to be removed from the record in order for it to be considered *de-identified*[8].

1.2 Infrastructure

A significant hurdle to sharing data is the agreement of the supporting technical architecture and infrastructure. Many attempts at data sharing require either (1) a centralized data source, or (2) the transmission of bulk data to other institutions. Both options introduce unique problems. Centralization increases the security risk footprint, and requires centralized trust in a single authority, while bulk data transmission forces institutions to yield operational control of their data.

1.3 Interoperability

Interoperability of healthcare records is the extent to which the clinical intent can be conveyed across institutional boundaries. Given the complexities of data in the healthcare domain, this is inherently difficult to achieve[9]. We examine interoperability within the context of two facets: *Structure* and *Semantics*, each necessary for the successful exchange of healthcare data[10].

Data structure, or the attributes and data elements use to convey information, is an important part of interoperability. Healthcare data is complex, and heterogeneous structures decrease the effectiveness of analysis and reduce understandability. To combat this, several industry-wide standards have been advanced[11]. While effective, there is no one authoritative standard, and aligning data encoded with disparate standards is a non-trivial task.

Semantics refers to the use of terminologies and vocabularies to describe data meaning, or to *codify* the data. This codification of healthcare data is important to its interpretation, but is only effective if all parties agree upon the same codification schemes, or *controlled terminologies*[12]. Often, subsets of vocabularies are used to scope a particular domain of interest. These subsets, called *Value Sets*, may be used in conjunction with structural models to constrain the allowable codifications for attributes or attribute types.

2 Goals

The main goal of this work is to describe an approach to effectively and securely share healthcare information within a data sharing network. We believe that a patient's record should be consistent and available across institutional boundaries, and the terms of its access strictly dictated by the patient. As a secondary goal, this data should not only be shared, but shared in such a way that all interested parties can understand the structure and meaning, ultimately leading to improved data utility and patient care.

3 Proposal

3.1 Assumptions

Below are general assumptions about healthcare stakeholders (or *nodes*) participating in a data sharing network. These assumptions exclude any regulation/incentives that the network itself defines.

1. There is value in receiving external data from other nodes, but only if you can understand the data structure and semantics.
2. Without guarantees of security and auditability, nodes will neither share nor receive data.
3. The patient ultimately controls their record, and authorizes who may access it and when.

3.2 Background

3.2.1 Blockchain

A *blockchain* is a distributed transaction ledger[13]. The blockchain itself is composed of *blocks*, with each block representing a set of *transactions*. As a data structure, a blockchain has several interesting properties. First, blocks are provably immutable. This is possible because each block contains a *hash*, or numeric digest of its content, that can be used to verify the integrity of the containing transactions. Next, the hash of a block is dependent on the hash of the block before it. This effectively makes the entire blockchain history immutable, as changing the hash of any block $n - i$ would also change the hash of block n.

The blockchain itself does not depend on a central, trusted authority. Rather, it is distributed to all nodes participating in the network. Because no centralized authority may verify the validity of the blockchain, a mechanism for reaching network consensus must be employed. In Bitcoin, a *Proof of Work* function is used to ensure network consensus[13]. This strategy requires that any node wishing to add a block to the blockchain must complete a computationally expensive (but easily verifiable) puzzle first. At a high level, this ensures consensus of the network because there is an opportunity cost (the computation time) to building a block. There are several other techniques used, such Proof of Stake[14] and Proof of Activity[15], but all are designed to drive the network to consensus on blockchain validity.

Miners are nodes that assemble the blocks and add them to the blockchain. It is through the miners that the consensus strategy is enacted, usually via some incentivisation protocol. In Bitcoin, for example, miners are incentivized by collecting transaction fees and also by a reward for adding the block to the blockchain. In general, however, there should exist an incentive for them to only build on top of valid blocks, which in turn drives the entire network to consensus.

3.2.2 Fast Healthcare Interoperability Resources

Fast Healthcare Interoperability Resources (FHIR)[16, 17, 18, 19] is an emerging standard that depicts data formats and elements, along with providing publicly accessible Application Programming Interfaces (APIs) for the purpose of exchanging Electronic Health Records. The standard was created and is managed by the Health Level Seven International (HL7) healthcare standards organization. FHIR is licensed without restriction or royalty requirements, which should serve to further facilitate its broader adoption. FHIR offers the potential for increased utilization of mobile and cloud-based applications, medical device integration, and flexible/customized healthcare workflows. FHIR enables the separation of EHR data elements into defined structured data types known as *resources*. Two of the resource types pertain to identification (providers and patients) and common clinical activities. The segmented resource constructs of FHIR facilitate the transfer of portions of EHR data where appropriate or desired. FHIR resources follow Representational State Transfer (ReST)[20] principles, and can be validated for structural conformance to the standard as well as further refined by additional conformance statements called *Profiles*.

3.3 A Healthcare Blockchain

Because a blockchain is a general-purpose data structure, it is possible to apply it to domains other than digital currency. Healthcare, we believe, is one such domain. The challenges of a patient record are not unlike those of a distributed ledger. For example, a patient may receive care at multiple institutions. From the patient's point of view, their record is a single series of sequential care events, regardless of where these events were performed. This notion of shared state across entities, inherent to the blockchain model, is congruent with patient expectations. Also, it is reasonable to assume that each patient care event was influenced by one or more events before it. For example, a prescription may be issued only after a positive lab test was received. The notion of historical care influencing present decisions fits well into the blockchain model, where the identity of a present event is dependent on all past events.

Figure 1 describes the structure of a block of healthcare data. Much like the Bitcoin approach, our block is a Merkle Tree-based structure[21]. 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 FHIR Resources 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. FHIR was chosen as a exchange format not only because it is an emerging standard, but also because it contains inherent support for provenance and audit trails, making it a suitable symbiotic foundation for blockchain ledger entries. FHIR in conjunction with the blockchain can serve to preserve the integrity and associated context of data transactions.

A transaction has the following characteristics:

- **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 URI of the FHIR Profile to which this resource conforms.
- **Secure Index:** An encrypted index allowing for data discovery without leaking information about the record. See Section 3.6 for more information.

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, which is discussed in section 3.5.

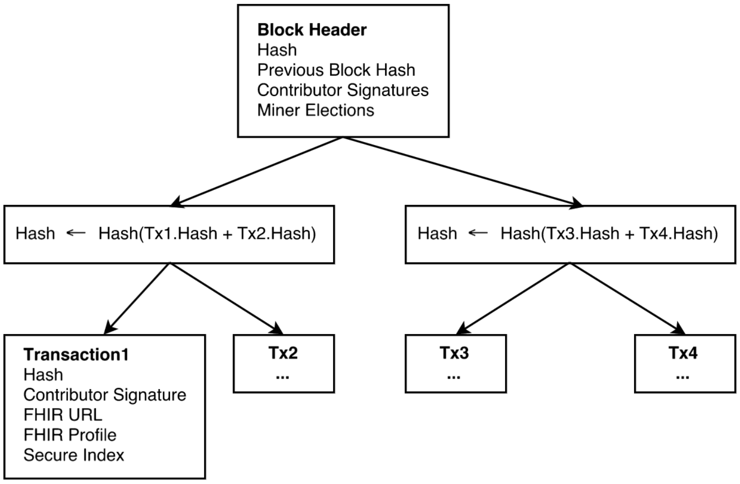

Figure 1: A healthcare blockchain block containing entries into the patient record.

3.4 Adding Data to the Blockchain

Figure 2 outlines the basic activities involved in adding data to the blockchain. In our system, much like Bitcoin, a block is added to the blockchain at regular intervals of time. For Bitcoin, this interval is determined by the difficulty of the Proof of Work function. For our network, we specify a constant interval of time for creating a block, or a *block period.* Within this block period, the network undergoes four phases of activity. First, during the *Transaction Distribution* phase starting at time T_α, 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. 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. The miner node then adds the block to its local blockchain, and finally distributes the new blockchain in the last phase, *New Blockchain Distribution.*

Algorithm 1 describes this process in more detail. Transactions are collected starting at line 3. Note that the miner cannot mine its own transactions, as shown in line 4 where it is excluded from the set of nodes N. When signing the block, only nodes with at least one transaction in the block are required to sign. This computation is shown in line 7. At the end of this algorithm, the blockchain is distributed to all nodes.

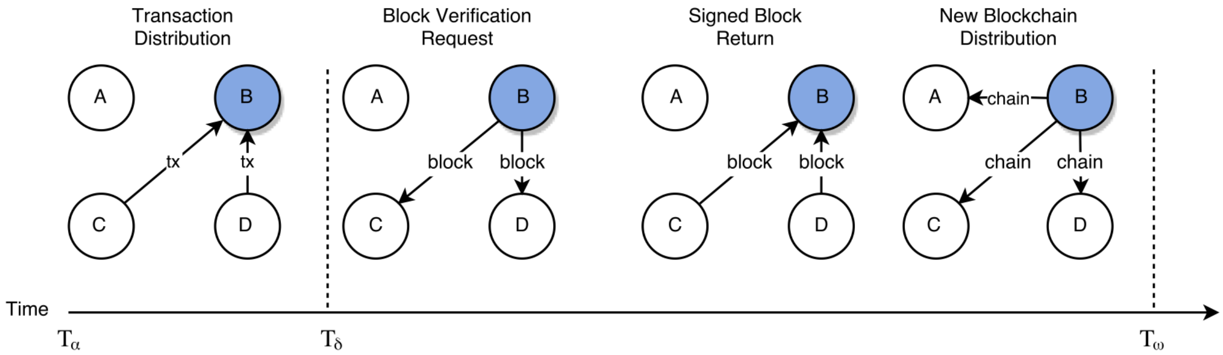

Figure 2: The four phases of adding a block to the healthcare blockchain.

Algorithm 1: Creating a new block and adding it to the blockchain.

```
input   : A set $N$ of Nodes participating in the network.
input   : A blockchain, $B$ representing a sequence of $\{b_0...b_n\}$ where $b_n$ is the current (last) block
          on the chain.
input   : $T_\delta$, the end of the Message Distribution phase.
$\alpha \leftarrow$ ElectMinerNode($b_n, N$);
$P \leftarrow \{\}$;  //Begin with an empty set of pending transactions.
while CurrentTime() $< T_\delta$ do
    foreach $n \in N - \{\alpha\}$ do
        $P \leftarrow P \cup$ GetTransactionsFromNode($n$);
$b_\beta \leftarrow$ AssembleBlock($P$);
$N' \leftarrow \{n \in N | (\exists t)[t \in P \wedge$ IsOriginator($n$,$t$)$]\}$; //$N'$ is all nodes with $>= 1$ transaction.
foreach $n \in N'$ do
    SignBlock($b_\beta, n$);
$B' \leftarrow$ AddBlock($B, b_\beta$)
foreach $n \in N$ do
    DistributeBlockchain($B', n$);
```

3.5 Mining

We use the term *Mining* to refer to adding blocks to the blockchain. The general intent is similar to that of Bitcoin, but our use case demands a substantially different approach. An overarching goal of the network is to avoid a Proof of Work model, where network computational power is expended without providing something intrinsically valuable. Rather, we aim to arrive at network consensus by forcing nodes to provide proof that the data a transaction references can be meaningfully interpreted, while at the same time requiring nodes to verify these validity proofs. This mechanism, described below, not only ensures blockchain consistency, but incentivizes interoperability among the nodes.

3.5.1 Proof of Interoperability

Proof of Interoperability is an alternative method for network consensus that avoids some of the of disadvantages of Proof of Work. Specifically, it 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 our use case, 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.

Algorithm 2 describes the process in greater detail. 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 `CheckProfileConformance` function. This operation will use the `FHIR URL` to make a `validate`[1] 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.

```
Algorithm 2: Proof of Interoperability.
input  : A set $P$ of pending transactions.
input  : A set $F$ of network agreed-upon FHIR Profile URIs.
input  : $b_\beta$, the current block being assembled.
output : A set $V$ of valid transactions.

$V \leftarrow \{\}$;  //Begin with an empty set of valid transactions.
foreach $t \in P$ do
    $u \leftarrow$ GetFhirURL($t$);
    $p \leftarrow$ GetFhirProfile($t$);
    if $p \in F$ then
        $result \leftarrow$ CheckProfileConformance($u$,$p$);  //Using the FHIR 'validate' operation.
        if Conforms($result$) then
            $V \leftarrow V \cup \{t\}$;
```

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. This type of collaboration necessitates a centralized, well known repository. For the value sets, we propose the use of the Value Set Authority Center (VSAC)[22] as a value set repository.

3.5.2 Miner Election

In a Proof of Work scenario, miners compete for the right to add a block to the blockchain. We instead employ a system of guaranteed *mining share*, similar to the system employed by MultiChain[23]. This system has several advantages. First, nodes know at the start of the block period who the next miner will be, so transactions may be sent directly instead of distributed to the entire network. Next, it ensures that the mining work required to keep the network consistent is distributed evenly. Finally, by eliminating the competition of Proof of Work, we eliminate wasted computational effort.[2]

The Miner Election process is described in Algorithm 3. Recall that the last step of adding a block to the blockchain is for the participating nodes to sign it (see Algorithm 1). During this signing process, each node is required to submit a random number to be used for miner election. This set of random numbers is collected on line 1, and is hashed together with the block hash to produce a new number. The next miner then becomes the node whose Public Key is closest to this value. This process serves two purposes: (1) The probability of becoming a miner for any node in the network N should be $1/|N|$, and (2) the random number used for election is seeded by all participating nodes in the network. This prevents a node from generating a non-random number and electing itself or a chosen collaborator.

[1] https://www.hl7.org/fhir/resource-operations.html#validate

[2] We do not assert that Proof of Work effort is strictly *wasted*. The work expended by nodes in a Proof of Work system certainly has value, as it is the mechanism by which the network stays consistent.

Algorithm 3: Miner Election.

```
input   : A set $N$ of Nodes participating in the network.
input   : The current (last) block on the blockchain, block $b_n$.
output  : A randomly elected miner node $\alpha$.

$S \leftarrow$ GetRandomSeed($b_n$);
$h \leftarrow$ GetBlockHash($b_n$);

foreach $s \in S$ do
    $h \leftarrow$ Hash($h + s$);

$\alpha \leftarrow$ where $|$GetPublicKey($n$) $- h|$ is minimized for node $n$;
```

3.6 Data Discovery and Access

Even though the block itself does not contain the actual record data, searchability and discoverability remain requirements, as well as a mechanism to access data once the appropriate transactions are found. External entities, with the appropriate permissions, may query the blockchain using keywords in the `Secure Index` field of the transaction. These keywords may be encrypted to prevent data leakage while still being searchable[24, 2]. Once the transactions of interest are located, the `FHIR URL` can be used to retrieve the actual resource.

3.7 Security

As stated above, data security (both privacy and anonymity) are fundamental priorities for the system. A multi-faceted approach to security for our proposed network includes:

Blockchain Encryption. Nothing in the blockchain should be stored in plain text. *Public* information, or information intended for all nodes in the network, is expected to be encrypted by a network-shared key, while sensitive information should be encrypted by the originating node.

Privacy Preserving Keyword Searches. To facilitate data searchability and discoverability, Privacy Preserving Keyword Searches[24] are used. In this way, an external entity may request a set of transactions from the blockchain matching some criteria, with both the query and the transactions remaining encrypted.

Smart Contracts. In reality, the security landscape around the patient record is much more nuanced than simply encrypting data. Patients may authorize access to their record only under certain conditions or for a specific reason. This notion of the codification of usage agreements is called *smart contracts*[25]. There is precedent for their use on a blockchain (e.g., the Ethereum project[26]), and given the complexities involved with our healthcare use case, smart contracts will play an important role. The intent is to ensure that patient authorization is codified and executable – for example, a patient may want their data shared only for research of a certain type, or for a given time range. These smart contracts can be placed directly on the blockchain as transactions[27], providing not only assurances of validity but an audit mechanism as well.

3.8 Patient Identification

Consistently identifying a patient between institutions is a non-trivial problem. Many approaches involve some variation of a centralized Master Patient Index (MPI)[28], or a single trusted identifier source. This approach has many of the same disadvantages as centralizing patient data – mainly, it requires centralized trust and consolidates valuable information in a single, known place. While a robust MPI discussion is beyond the scope of this work, we can apply some of the design approaches used here. Borrowing from the Bitcoin model, we can think of data on the blockchain assigned to *addresses*, not patients, with patients controlling the keys to these addresses. The advantage to this approach is that consensus on a single identifier does not need to be reached – a patient may hold multiple blockchain addresses for different institutions. This notion requires the patient to manage and maintain keys to these addresses via an electronic *wallet*, and is a significant deviation from current practices where institutions assign and own patient identifiers.

4 Business Value

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[5] 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* – meaning, 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.

5 Summary

The challenges of data sharing within the healthcare domain are significant. Simply sharing data is not enough – we've shown that effective data sharing networks require consensus on data syntax, meaning, and security. We've proposed that a blockchain can play a fundamental role in enabling data sharing within a network, and have defined the high level structures and protocols necessary to apply this new technology to healthcare. Building on techniques used successfully by other blockchain applications, we've introduced a new consensus algorithm designed to facilitate data interoperability. Finally, we have applied extra measures of security on the blockchain such as network-wide keys and smart contracts, keeping security a top priority. Ultimately, we believe that a blockchain-based data sharing network is a tenable solution for the complex problem of sharing healthcare data.

6 Future Directions

6.1 Aggregate Blockchains

In this work, we've explored how nodes in a data sharing network may interact. Intuitively, we can conceptualize these nodes as individual institutions or providers. This mental model aligns to current Heath Information Exchanges, which tend to be (at least in the United States) groupings of regional providers[29]. But what if we reconsider our definition of a node in the network? Envision a node not as a single institution, but as an entire blockchain-based data sharing network. We can now imagine not only cross-institutional sharing, but cross-network sharing as well. This would enable the institution/provider-based networks to grow and evolve, at the same time allowing them to connect to similar networks. This notion of aggregation, or *nested blockchains*, may be an approach to extending the reach of collaborations and sharing beyond local networks.

6.2 Machine Learning

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 `DiagnosticReports` of radiology images to the blockchain. An AI service provider that specializes in developing novel machine learning algorithms with which the hospital has partnerships would be allowed to run their algorithm over the images and publish the AI diagnosis 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. The blockchain also provides an irrefutable trail of what the AI provider diagnosed and the final official diagnosis.

References

[1] Yaorong Ge, David K Ahn, Bhagyashree Unde, H Donald Gage, and J Jeffrey Carr. Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations. *Journal of the American Medical Informatics Association*, 20(1):157–163, 2013.

[2] Chris Clifton, Murat Kantarcioğlu, AnHai Doan, Gunther Schadow, Jaideep Vaidya, Ahmed Elmagarmid, and Dan Suciu. Privacy-preserving data integration and sharing. In *Proceedings of the 9th ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery*, pages 19–26. ACM, 2004.

[3] Joshua R Vest and Larry D Gamm. Health Information Exchange: persistent challenges and new strategies. *Journal of the American Medical Informatics Association*, 17(3):288–294, 2010.

[4] Paul C Tang, Joan S Ash, David W Bates, J Marc Overhage, and Daniel Z Sands. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of the American Medical Informatics Association*, 13(2):121–126, 2006.

[5] Jan Walker, Eric Pan, Douglas Johnston, Julia Adler-Milstein, et al. The value of health care information exchange and interoperability. *Health Affairs*, 24:W5, 2005.

[6] Randolph C Barrows and Paul D Clayton. Privacy, confidentiality, and electronic medical records. *Journal of the American Medical Informatics Association*, 3(2):139–148, 1996.

[7] Centers for Disease Control, Prevention, et al. HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services. *MMWR: Morbidity and Mortality Weekly Report*, 52(Suppl. 1):1–17, 2003.

[8] US GPO. CFR§ 164 security and privacy. 2008. http://www.access.gpo.gov/nara/cfr/waisidx_08/45cfr164_08.html. Accessed: 2016-08-06.

[9] Charles N Mead et al. Data interchange standards in healthcare it-computable semantic interoperability: Now possible but still difficult. do we really need a better mousetrap? *Journal of Healthcare Information Management*, 20(1):71, 2006.

[10] Amit P Sheth. Changing focus on interoperability in information systems: from system, syntax, structure to semantics. In *Interoperating Geographic Information Systems*, pages 5–29. Springer, 1999.

[11] A Begoyan. An overview of interoperability standards for electronic health records. *USA: Society for Design and Process Science*, 2007.

[12] James J Cimino et al. Desiderata for controlled medical vocabularies in the twenty-first century. *Methods of Information in Medicine-Methodik der Information in der Medizin*, 37(4):394–403, 1998.

[13] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[14] Sunny King and Scott Nadal. PPCoin: Peer-to-peer crypto-currency with proof-of-stake. *Self-Published Paper, August*, 19, 2012.

[15] Iddo Bentov, Charles Lee, Alex Mizrahi, and Meni Rosenfeld. Proof of activity: Extending bitcoin's proof of work via proof of stake. *ACM SIGMETRICS Performance Evaluation Review*, 42(3):34–37, 2014.

[16] HL7. HL7 Fast Healthcare Interoperability Resources (FHIR). https://www.hl7.org/fhir/. Accessed: 2016-08-01.

[17] Russell Leftwich. The path to deriving clinical value from FHIR - InterSystems. http://www.intersystems.com/library/library-item/path-deriving-clinical-value-fhir/. Accessed: 2016-08-06.

[18] iNTERFACEWARE Inc. What is 'FHIR' and why you should care? . http://www.interfaceware.com/blog/what-is-fhir-and-why-should-you-care/. Accessed: 2016-08-06.

[19] Tim Benson. *Principles of health interoperability HL7 and SNOMED*. Springer Science & Business Media, 2012.

[20] Roy Thomas Fielding. *Architectural styles and the design of network-based software architectures*. PhD thesis, University of California, Irvine, 2000.

[21] Leslie Lamport. Constructing digital signatures from a one-way function. Technical report, Technical Report CSL-98, SRI International Palo Alto, 1979.

[22] Olivier Bodenreider, Duc Nguyen, Pishing Chiang, Philip Chuang, Maureen Madden, Rainer Winnenburg, Rob McClure, Steve Emrick, and Ivor DSouza. The NLM Value Set Authority Center. *Studies in Health Technology and Informatics*, 192:1224, 2013.

[23] Steffan D Norberhuis. *MultiChain: A cybercurrency for cooperation*. PhD thesis, TU Delft, Delft University of Technology, 2015.

[24] Yan-Cheng Chang and Michael Mitzenmacher. Privacy preserving keyword searches on remote encrypted data. In *International Conference on Applied Cryptography and Network Security*, pages 442–455. Springer, 2005.

[25] Nick Szabo. Formalizing and securing relationships on public networks. *First Monday*, 2(9), 1997.

[26] Vitalik Buterin. A next-generation smart contract and decentralized application platform. *White Paper*, 2014.

[27] Loi Luu, Jason Teutsch, Raghav Kulkarni, and Prateek Saxena. Demystifying incentives in the consensus computer. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 706–719. ACM, 2015.

[28] Peter Littlejohns, Jeremy C Wyatt, and Linda Garvican. Evaluating computerised health information systems: hard lessons still to be learnt. *BMJ*, 326(7394):860–863, 2003.

[29] Ashish K Jha, David Doolan, Daniel Grandt, Tim Scott, and David W Bates. The use of health information technology in seven nations. *International Journal of Medical Informatics*, 77(12):848–854, 2008.