Implementating Cross-Enterprise Document Sharing (XDS.b) based on Blockchain Technology

Petnathean Julled   
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

Assadarat Khurat  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

Pattanasak Mongkolwat  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

*Healthcare information sharing and interoperability between healthcare organizations are important factors to healthcare quality and safety since a patient may require medical services and consultations from different healthcare providers. Many challenges inhibit successful data sharing such as data integrity, security, and privacy. Integrating Healthcare Enterprise (IHE) provides Cross-Enterprise Document Sharing (XDS.b) profile that allows the adopted organizations to share health documents between institutions. No specific security implementations were endorsed, which allows latest security technologies to be applied. Healthcare domain has become a major target in emerging cyber-security threats. These threats increase difficulty to maintain secure health information sharing network. These cyberthreats can compromise integrity and availability of data and effect patient’s life. Blockchain technology can be used to solve health information sharing issues. A novel method using Blockchain technology to ensure health information integrity and availability is implemented, demonstrated and freely available(?), allowing health document sharing through decentralized network while addressing cyber-security issues through unique characteristics of Blockchain technology.*



Keywords—health information, interoperability, information sharing, information security, blockchain, smart contract, ihe, xds

# Introduction

The increasing demand for better quality and secure healthcare services and operation efficiency play an important role in patient services and economic outcomes. Healthcare information sharing and interoperability between healthcare organizations are one of the major solutions to improve healthcare service quality. Patient’s health documents are scattered across different healthcare organizations, which may cause by different medical services being offered by different providers. Each healthcare provider has its own methods, processes, and workflow to handle healthcare information. This makes it harder for one health information system to interoperate with one another. Sharing health information with trusted parties who may not employ the highest level of security standards and practices exposing vulnerabilities to patients, businesses, and organizations. The risk-reward ratio from sharing patients’ information with others may not be worthwhile if it were done improperly. This creates high friction for one organization to share their information with each other. It is even more difficult for individual patients to integrate and share their health information with different providers. These interoperation problems cause a huge decrease in efficiency in healthcare operations and result in a lower quality of healthcare service [1–8]. Therefore, there are many initiatives [9–14] that start to standardize healthcare information technology with the goal to allow healthcare organizations to be able to exchange patients’ information with one another. By applying Blockchain technology to the Cross-Enterprise Document Sharing (XDS.b) Profile created by Integrating Healthcare Enterprise (IHE), the concept can help healthcare organizations achieve both secure health information sharing and interoperability between organizations. Decentralization from Blockchain passively allows the distribution of data via Blockchain-specific protocol to the network without the need for a centralized mediator. Transparency and cryptographic nature of Blockchain characteristics establish an environment that allows each stakeholder to share health information with each other without requiring trust between each party as no one can have absolute authority over shared data and preventing tampering existing data. Combining Blockchain with XDS.b will significantly reduce data sharing risks even the sharing party does not deploy the highest level of security standards and practices. Concurrently, decentralization of data also opens opportunities for the development of a patient-centric application which may further allow each individual to integrate, share, and keep track of their own healthcare information at its best.

Besides the issue regarding health information sharing between different enterprises, emerging cyber-security threats have been threatening healthcare domain. Hospitals have been hit by ransomwares interrupting medical operations and severely disrupt healthcare services.. The number of patient records breached has been on an increase every year from 2012 to 2020 [15–19]. Security experts estimated the number of ransomware attacks on healthcare institute to be close to 1,000 per day in 2015, which is 35% more than the previous year. The number even rose to 4,000 attacks on certain days according to a report published by Symantec in 2016. The case when Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak [20] shows that failing on secure integrity and availability of healthcare information cause a major disruptive factor on continuity of medical operations. Assumed that organization policy and employee security awareness about cyber-security were addressed, there are several techniques proposed to mitigate the problem. One of major solution being propose is utilization of Blockchain technology on healthcare information or its infrastructure. Cryptographical components and consensus mechanism of Blockchain will give immutable characteristic and secure integrity of the information, while decentralization of published data help secures its availability [21–24].

Blockchain can be informally defined as a distributed digital ledger of cryptographically signed transactions that are grouped into blocks. [25] Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledgers within the network, and any conflicts are resolved automatically using established rules. This gives its characteristics to sustain threat against integrity and availability of information. At the same time, with consensus as vital part of Blockchain, it allows members of Blockchain network to systematically “trusted” each other without the need of mutuality trust or physical agreement. Additionally, as distributed decentralized network, Blockchain requires each member to passively share information with each other. Since the introduction of the first Blockchain based cryptocurrency named ‘Bitcoin’, there are many Blockchain platforms and service providers entered the industry. One of major platform adopt by many kinds of applications is Ethereum. It was the first major platform that introduce usage of Blockchain for various fields of applications other than cryptocurrency with its ‘Smart-contract’. It allows developers to publish logic models or computational algorithms into Blockchain which enables a while variety of usage for the technology [26,27].

As for addressing issues regarding health information sharing between different enterprises, there are concepts of utilizing Blockchain proposed by Mayo Clinic and “MedRec” MIT. Both introduce an effective way with potential to utilize Blockchain technology for information sharing in healthcare enterprise environment. The works have given great demonstration of how decentralization offered by Blockchain can resolve trust issue where each enterprise require “trust” before beginning to share their information with others. However, both solutions are not yet directly introduced how Blockchain can help mitigate cyber-security threats threatening integrity and availability of data in healthcare domain. In this work, we propose a solution that can solve data integrity and availability issues while help reduce the friction of allowing health document sharing between different enterprises by utilizing Ethereum’s Smart-contract to enable implementation of IHE XDS.b Profile concept with Blockchain.

The next section provides information about relevant works that inspire our design, following with background knowledge which our work is based on in section III. Then, we move into the detail of design method in section IV before dive into implementation techniques in section V. At last, we conclude the proposed concept in in section VI and end with discussion of this work in section VII.

# RELATED WORK

## A Blockchain-Based Approach to Health Information Exchange Networks [28]

Kevin Peterson et al. from Mayo Clinic proposed the concept that using Blockchain as a medium for health information exchange network. The work utilizes Fast Healthcare Interoperability Resources (FHIR) protocol as a gateway which allows members of the network to access health information from each other, while ensure distribution of accessibility within the network by published those gateways to Blockchain. Every activity on the network will be recorded on the Blockchain providing audit trail for the network. They proposed several concept ideas about using computational resource within Blockchain network in the more meaningful way contribute to healthcare environment. Additionally, the work also included several suggestions about Blockchain component that may provide more compatibility of the technology for healthcare information environment. In this work, we adopt the idea of using Blockchain as a medium for health information exchange network and several suggestions provided, that should make Blockchain technology more compatible with healthcare information environment. However, the work did not mention about how Blockchain technology can be beneficial for health information sharing in term of cyber-security.

## “MedRec” prototype for electronic health records and medical research data

MedRec [24] was proposed as a prototype for electronic health records by utilize Ethereum’s smart-contract to contain metadata about the record ownership, permissions and data integrity represent existing medical records that are stored within individual nodes on the network. The concept helps reduce barriers to effective data sharing addressing interoperability issue caused by economic incentives that encourage “health information blocking”. At the same time, their proposal also benefits as the source of medical research data, by providing anonymized healthcare data for research institutions in the form of Blockchain participation reward. Their Blockchain implementation focus on addressing four major issues for health information exchange included: fragmented data which also slow access to medical data, system interoperability, patient agency, and improved data quality and quantity for medical research. Additionally, as MedRec was built on the work of Zyskind et al. [29]. They utilized some cryptographical characteristics of Blockchain to provide accessible “bread crumb trail” which allows data user to trace back medical history to improve operation efficiency. From MedRec, we adopt the concept of using Ethereum’s smart-contract to contain essential information that allow ability to discover data within Blockchain network. However, the concept may require overhaul and rework on the whole system for adoption which may not be affordable in some cases, like the organization may have limited resources or recently invested most of their available resources on making their system comply with existing health information sharing standard.

# BACKGROUND KNOWLEDGE

## Cross-Enterprise Document Sharing (XDS.b) Profile from Integrating Healthcare Enterprise initiative (IHE)

Modern medical operation has large amount of healthcare information flow within the system. Throughout the age, many medical service providers and organizations have developed their own health information system and database to increase efficiency of operation in their medical services. As the time past, information of individual patients has scattered amongst different systems. This becomes a new challenge for healthcare enterprise to further enhance their medical service efficiency by sharing health information with other systems within healthcare industry domain

IHE is an initiative by healthcare professionals and industry to improve the way health information systems in healthcare integrate and share information. IHE promotes the coordinated use of established standards such as HL7 and DICOM [14] to address specific clinical needs in support of optimal patient care. Systems developed in accordance with IHE integrate and communicate with one another better, are easier to implement, and enable healthcare providers to use information more effectively. This helps enable seamless health information that is usable whenever and wherever needed. An IHE profile provides use of existing standards, specifications, tools, and services for interoperability. IHE also engages clinicians, health authorities, industries, and users to develop, test, and implement standards-based solutions to vital health information needs. [9] IHE provides convenient and reliable way of specifying a level of compliance to standards enough to successfully reach efficient interoperability.

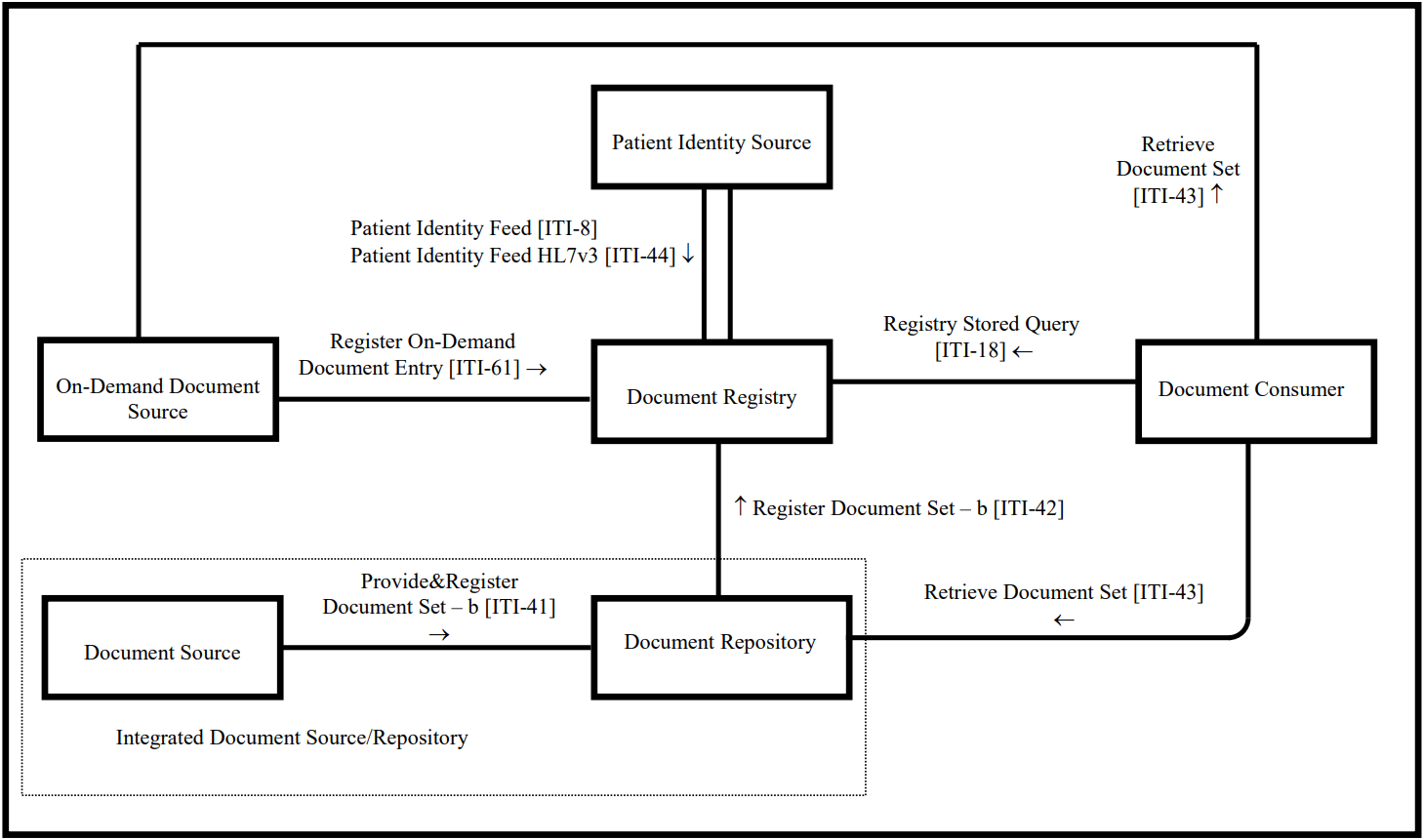


Figure 1 Cross-Enterprise Document Sharing – Set b [30]

Amongst many profiles created by IHE, there is one major profile that serve to improve efficiency of health information sharing between different enterprises called “Cross-Enterprise Document Sharing Profile (XDS.b)” [30] (Figure 1. Not should if you need to show this?). The main goal of XDS.b profile is to allow enterprises that being a member of health document sharing network (called “XDS Affinity Domain”) to discover shared health documents stored in the system of other institutions via central registry (named “XDS Document Registry”). The XDS Document Registry registers set of META-data attributes belong to each health documents to allow health information system to discover existing health document that stored within other organizations and able to systematically access the document using the information provided by META-data attributes. By specified format of transactions and method for each system to communicate with each other, XDS.b makes sure that all the systems within the network can communicate with each other in the same way. This allows document consumer and user in the network to share health documents with each other and put it to use as needed efficiently.

In Figure 1, each XDS “Actor” represents machine or software which takes the role in XDS.b Profile. Health document and its META-data attributes initially generated from Document Source Actor such as X-ray machine, physicians’ EMR terminal, etc. The generated documents and their META then store in Document Repository Actor via Provide & Register Document Set-b [ITI-41] transaction. The actor mostly referred to database or server which keep health documents available and ready for usage in healthcare operation. After that, Document Repository Actor register META-data attributes of stored document to Document Registry Actor via Register Document Set-b [ITI-42] transaction. The META-data attributes will contain information essential for Document Consumer Actor to discover health document available within XDS Affinity Domain and enable interoperability between corresponding software. Document Consumer Actor queries for information of registered document in Document Registry Actor via Registry Stored Query [ITI-18] transaction. Document Registry then returns query result to Document Consumer Actor via transaction following ITI-18 format. Eventually, Document Consumer Actor use information provided by query result to retrieve the document from its repository using Retrieve Document Set [ITI-43] transaction. It is expected that Document Repository Actor response to the request by sending copy of the document back to the Document Consumer Actor. For On-Demand Document Source, it is equivalent to Document Repository Actor as both are where Document Consumer retrieve those documents they seek. The only different is that On-Demand Document Source acts as repository which will immediately generate a health document at the time of request as the document only represents its subject at the time, while document stored within Document Repository represents event in health operation that already ended. For Patient Identity Source Actor, the actor acts as assistant for XDS Affinity Domain to identify identity of the same patient within the domain whose can be represent differently in each enterprise. This actor may not be necessary if XDS Affinity Domain already have policy or agreement which regulates all enterprises in the domain must use the same identification to identify the same patient. With these XDS Actor and transaction deployed, it ensures that all enterprise within XDS Affinity Domain can achieve and share health documents with each other.

## Blockchain Technology

Blockchain technology is a method that applied cryptographic techniques to locally ensure integrity of data while rely on decentralization and consensus mechanism to ensure integrity and availability of all data existing in the network [25]. These cryptographical techniques include the one that form “Block” and another one that form “Chain”. In Blockchain, those data being published are small fragment of information that represent proof of action in its own application. Therefore, it calls a “transaction”. A set of transactions approach Blockchain network at the same period will be hashed together, imagine like put these transactions into the same box and label it with its hash value, formed a “Block”. Additionally, the hash value of each block also includes hash value of previously generated block cause formation of a “Chain”. Any attempt to modify content of published block will cause change in hash value of entire chain which trigger rejection from the network.   
Together with hash “chain”, the concept also relies on “decentralization” of data where copy of entire chain was kept by many participants of the network called “node”. Any node with the version of chain that has even a bit different from the majority in the network will be rejected and the node will be forced to adopt the version adopted by the majority. These two techniques form together to become “Blockchain” which prevents modification of published content and ensure integrity of data. This concept guarantee that no one can ever be able to modify any data existing in Blockchain. However, there still be able to add more Block into Chain by utilization of consensus mechanism [31].

Consensus mechanism invented to ensure that no one in the network can freely attempt to modify content of transaction before it being published inside Blockchain, whether by select a trustable node who will verify certain Block being publish to the chain or have majority of reliable node approve authenticity of newly formed Block [32]. Some consensuses like Proof of Work (PoW), require participant nodes (called “miner”) who wants to verify a Block to compete to solve mathematic puzzle. The winner will be able to verify the Block and get reward based on each network policy. As the puzzle requires each node to spend huge amount of computational resource, given randomness which make it nearly impossible for miner node to be able to get a hand on prefer Block and attempt suspicious activity during verification process [33]. On the other hand, some consensus mechanisms like Practical-Byzantine False Tolerance (PBFT), invented to allow Blockchain network with limited computational resource to select trustable validator. This kind of consensus use voting mechanism which sacrifice ability to welcome anonymous node for lesser computational resources required for maintaining Blockchain and increased in efficiency of verification process, that means it rely on the environment that most of the nodes are not corrupted [34]. These mechanisms enable transparency in publication and verification of transaction in Blockchain. Additionally, the network also needs compatible permission model for its member to maximize effectiveness of consensus mechanism. According to [25], Blockchain can be categorized into two main types based on its permission model which determines who can maintain blockchain ledger (i.e. publish block). Permissionless blockchain networks provide simplicity in scalability of the network by allowing anyone in the network to maintain blockchain ledger. At the same time, permissioned chain allows only selected member to maintain or even just to participate in the network which allows accountability and auditability of the network in exchange for simplicity in scalability. Permissioned blockchain networks may also be used by organizations that wish to work together but may not fully trust one another. They can establish a permissioned blockchain network and invite business partners to record their transactions on a shared distributed ledger. The transparency provides by Blockchain and consensus with suitable permission model then create a passive “trust” amongst the network as no one in the network have absolute right to rules and manipulate the network and its content at their own will [35].

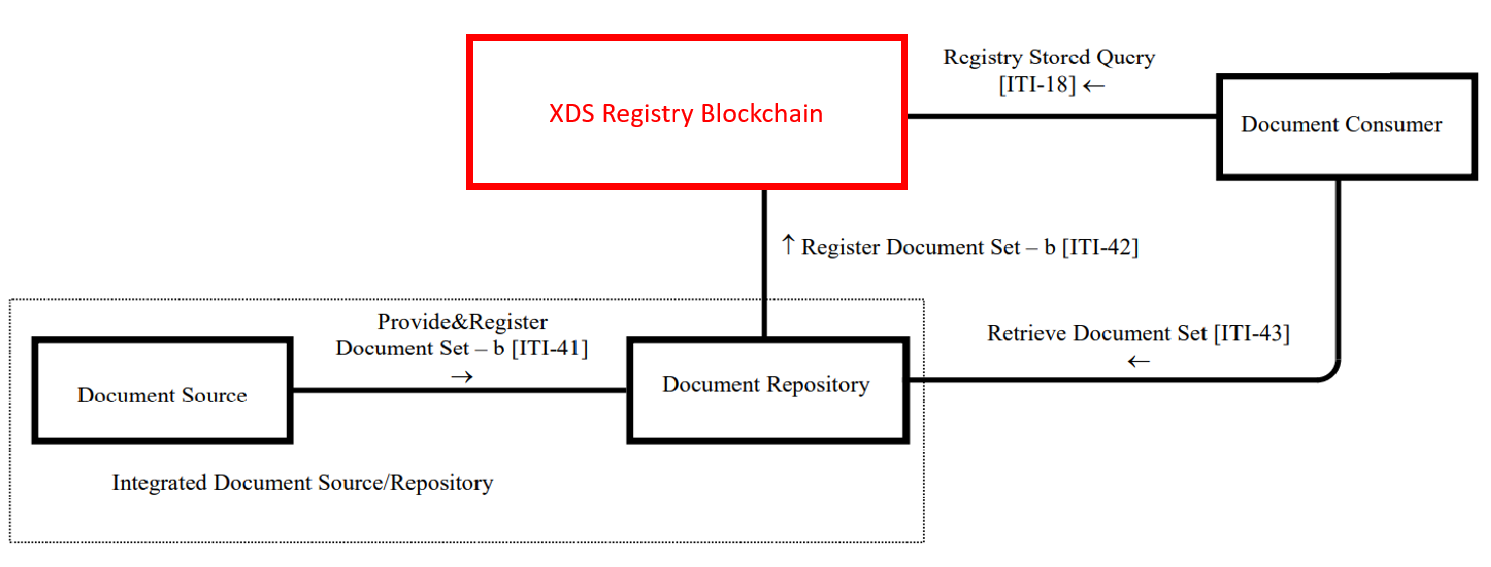
## Ethereum and Smart-Contract

Ethereum is one of the well-known open-source Blockchain platforms. The platform initially invented by a developer named Vitalik Buterin and further developed by the Ethereum community. The main approach of Ethereum Blockchain is about using Blockchain technology for applications other than cryptocurrency, i.e., create digital evidence for an actual contract between parties that can replace paperwork and cannot be deleted or tampered with, or act as digital evidence for supply chain tracing during transport and exchanging of goods. The platform proposed the concept of “smart-contract” [21,22]. Smart-contract allows developers to integrate their small-size computation algorithms or snippet of logic into Blockchain. This gives Blockchain characteristics [22] to those codes. Enable a wide variety of applications to work with Blockchain. The concept of smart contract later was adopted by other Blockchain platforms, created infinite possibilities of Blockchain application suitable with a variety of computational environment and usage. While each Blockchain platforms have their own technical methods for implementation, Ethereum’s smart-contract relies on JavaScript-like language called ‘Solidity’. The language invented to allow codification of human-understandable logic into programming language format understandable by ‘Ethereum Virtual Machine (EVM)’ named ‘JSON-RPC’. EVM represents a computational resource that shares amongst Ethereum network which allows machines with different environments to interact with Ethereum Blockchain without the need for specific computational environment or hardware. This allows Ethereum network to formed by wide variety of machines with different operation system and internal environment. At the same time, Ethereum Blockchain can adopt variety of consensus mechanism. The main Ethereum Blockchain initially adopted PoW. Due to limitation as it requires huge amount of computational resource to stay active, Ethereum network later forked the Blockchain line into several chain lines with different consensus. i.e. Proof of Stake and PBFT which adopt voting-like mechanism to allow reduction of computational resources consumption. As time passed, Ethereum community keeps on growing, now there are wide variety of consensus mechanism proposed to suit with different application and network environment.

# METHOD

This section describes a method of how we implement XDS.b Profile based on Blockchain technology. Start with a general use case scenario following with top view of the Blockchain network and consecutively narrowing into the design of XDS Blockchain, its components, and Smart-contract which took the main role to adapt the profile into the chain.

Figure 3 Replacing Document Registry Actor with XDS Registry Blockchain



## A Use Case Scenario

As shown in Figure 2, user at Hospital A needs to start with specifying value corresponding to XDS META-data attributes (Patient name, ID, etc.) that unique to the event specific for Mr.Bob and use it to search for associated registry using Document Registry Searcher program. Document Registry Searcher uses specified values to find for registered META-data attributes set in smart-contract. When matched, Document Registry Searcher returns the whole META-data attributes set of those matched one to the user at Hospital A. In this case, it may return more than one registry set that associated with Mr.Bob. User at Hospital A may need to seek for the one with latest timestamp or the one they needed to use. When the registry set was picked, they may need to use repository URI included in META-data attributes set to request for actual document in Hospital B. After that, Hospital B will response by allow Hospital A to access content of the document.

Due to unique nature of healthcare environment that emphasizes on confidentiality of data, this cause limit in implementation of the technology in the environment. Patient data cannot be put directly into Blockchain as it will become persistent by decentralization of Blockchain network as well as it will become more difficult to ensure confidentiality of data when its replica are distributed over the entire network [25], [36], [37]. We propose another approach to make the technology more compatible with implementation on healthcare information. IHE XDS.b Profile serves its purpose as central hub for health document exchange between different enterprises. This makes the profile best compatible with Blockchain technology as it will secure availability of health information exchange. In this implementation, we further extend the usability of the profile by allowing the organization that shared health documents from its source to act as data backup for the original by providing additional access points (URLs) for the document. This increases the survival chance of medical operation continuity when one organization compromised by ransomware as they may have a replica of data available on others in the network.

A

XDS  
Blockchain

B

Timeline

Search Mr.Bob registry

Return Mr.Bob registry

Request Mr.Bob’s document via contact info. provided by META in registry.

Return Mr.Bob document

Figure 2 Use case scenario flow chart

## Network Design

In our scenario, we declare that participants of the network are members of XDS Affinity Domain which assumes to be hospitals and healthcare institutions. Each member will need at least one computational machine to keep operate and maintain Blockchain ledger, thus becoming ‘Blockchain Node’. As the Blockchain allows only XDS Affinity Domain members to participate as node, so this Blockchain will be classified as permissioned chain. And for networking protocol between each node in the network, it relies on the adopted Blockchain platform invented by provider or community.

## Blockchain Components and Consensus

The main components of Blockchain comprise of the backbone engine which allows the network to form, operate, and maintain Blockchain ledger addition with consensus mechanism which maintain integrity of the network. In this work, we adopt Ethereum Blockchain platform as engine to operate components regarding cryptographical components forming ‘Block’ and ‘Chain’, Blockchain networking, actor identifying, transaction mapping, and maintaining the ledger. By ensure integrity of every ‘Block’ and ‘Chain’ identified by its hash value, this guarantees that no one can ever be able to modify anything published to Blockchain. This made all data within Blockchain to become persistent and always available to access if most of the network still exist. That means even if there are incident happened to one node, it will have no effect on the chain which is an advantage gaining from Blockchain compared to centralized database. Additionally, with the extend usage of XDS.b, the more times document got shared with node members mean the more alternative data backup for the source of the document. Even the source got compromised, they still have the document available to those network members who shared the document before the incident happened.

For consensus, it needs to be the consensus that can process large amount of Blockchain transactions at certain time due to continuous nature of medical operation and the loss of even single transaction is unaffordable. At the same time, it cannot be those mechanisms that consume excessive amount of computational resource from each node as most of participant will have limited resource to invest in Blockchain network. Combined with nature of permissioned chain which allow only selected participant to participate as node, this led the design to rely on consensus that based on majority of participant nodes are being reliable. i.e., PBFT. This kind of consensus require at least 2/3 of participant node to approve authenticity of transactions block being publish into the chain. The mechanism took the key role which guarantees that no one will be able to attempt modifying any publishing transaction before it entered the chain. The concept passively ensures that every data published in the chain was not differed from the original version introduced to the network by its owner. With these main components of Blockchain combined, it guarantees integrity of data from the moment it was introduced to the network until it successfully published into the chain as transaction and remain there as it became persistent and immutable in the network. All these mechanisms gave transparency in process of publishing data and keep it in the Blockchain, generate ‘trust by design’ for the network.

## Establish foundation of trust amongst the network

Foundation of ‘trust’ was formed from its core components in Blockchain. However, as strength of Blockchain rely on number of participants being reliable node, there still need a method to recruit new participants into the network. Blockchain participant nodes must be verified by member of the network before allowed to participate and interact with Blockchain. This can be done by establishing agreement or policy that requires the applicant to comply. It will vary depend on business model and common of interest amongst potential participant of the network. With an aid of ‘trust by design’, there are less factors to consider for joining the network in technical term. In this work, we assume that common of interest of the network is to be able to share their health document with each other using XDS.b Profile while ensure that the central registry created by the profile cannot be compromised by any kind of incident as if majority of the network was not affected. Then this allows the network to have health document sharing available even some amount of its members became victim to cyber incidents.

## Integrating Blockchain with XDS.b

In IHE ITI Technical Framework, they specified that XDS Document Registry actor who act as hub that registered all essential information about all health documents generated and kept by XDS Affinity Domain, should be a database that allows Document User to query for information of health Document they seek. The existing solution for the database is utilization of SQL or non-SQL centralized database. In this work, we propose replacing of these centralized databases with Blockchain ledger as shown in Figure 3. According to Figure 1, our Blockchain design will take the role of Document Registry. That means each Blockchain node will keep, operate, and maintain copy of Blockchain ledger that contains entire health document registry entry. Following guideline provided by IHE ITI Technical Framework, all nodes will receive ITI-42 transaction from its local Document Repository. The node then interprets the transaction and convert it into Blockchain transaction before broadcasting it to all nodes in the network via Blockchain protocol. At the same time, every node will interpret ITI-18 transaction from Document Consumer and query for information of health document via Smart-contract. For current work, we assume that ITI-61 transaction will be further implement to the Blockchain concept in the future. Additionally, we assume that patient identification was standardized amongst all the network beforehand, so it eliminates the need of ITI-44 transaction in our implementation. In summary, data content that going to be published into Blockchain is META-data attributes of available health document which specified information essential for health information sharing software complied with IHE XDS.b Profile to discover and retrieve document in other enterprise.

Compare to original Cross-Enterprise Document Sharing Framework (XDS Framework), we replaced traditional database for XDS Registry Actor with blockchain ledger. With blockchain applied, this new XDS Registry now gained blockchain characteristics. Immutability keep XDS Registry persist as the network still exist. All members within XDS Affinity Domain always have up-to-date version of XDS Registry as distributed characteristics of blockchain force every member to maintain the same copy of ledger at all time. With decentralization and consensus mechanism deployed, the blockchain network now gain transparency in Block addition process and can be guaranteed that no one have absolute right to manipulate transaction in blockchain at their own will. This given the foundation of “trust” which allows different healthcare enterprises to share their documents with each other even they are not fully trust one another. Additionally, to allow compatibility of new XDS Registry to be able to operate with existing XDS transaction of XDS Framework, we also implemented XDS transactions interpreter to act as the middle between original framework and blockchain. This allow our new XDS registry blockchain to work almost seamlessly with existing system currently complied to XDS Framework.

## XDS Blockchain and Smart-contract Design

As shown in Figure 4, Smart-contract will be the main component that takes the role to keep all set of META-data attributes containing information of existing health document in the network Each set of information differentiated by characteristics of its original document, within Blockchain ledger. When Document Registry Searcher program was triggered by ITI-18 transaction, it will perform iteration search on all META-data attributes set existing on the chain. All matched set will return as query result to Document Consumer as a list for its user to pick the one they needed. After the user picked the set they needed, user-side program within Document Consumer will trigger Smart-contract to return the whole set of META-data attributes of the selected set. Eventually, user-side program will use information provided by retrieved META-data attributes to access actual document in its repository in document owner hospital.

## An augmentation to mitigate data-corruption incident

In original XDS Framework, the sole purpose of the framework is to allow health document sharing between different enterprises. In this work we also propose utilization of Blockchain technology to further help in mitigation against data-corruption incident like ransomware or wipe-ware. It is almost impossible that one organization can absolutely guarantee that they will not be affected by any cyber-incident forever so, a data backup will always be needed to ensure the availability of data to allow continuity of operation even if the organization was hit by cyber-incidents. Our implementation allows an alternative investment in data backup by allowing other node members who shared the document to act as decentralized data backup driven by the need for health information sharing. That means the document source may need lesser investment on their data backup to secure availability of the data while achieving the benefit of document exchange for increasing in healthcare operation performance. This can be done by requiring those members node to use their XDS Repository to act partially as data-backup for one another in the blockchain network. After certain nodes have retrieved a copy of the health document from another node using the information provided in the XDS Registry. XDS Repository of the node with a replica of shared health document simply needs to update additional access pathway for the copy into the registry of the original document within XDS Registry (shown in Figure 5) as to provide an alternative pathway to access the document. By doing so, even the original repository affected by data-corruption incident and lost data of the original document, there still have alternative pathways to access copy of the document available. Consider healthcare operation which requires huge amount of health information sharing by nature, a lot of available alternative pathway for health document can be expected in actual deployment. This concept will help member of the network in better mitigation against raising cyber-incident that cause data-corruption. The more they share their information with other, the more alternative copy of certain health document become available. This concept further motivates the network to maintain XDS Blockchain and share their health document with one another, empowering healthcare industry and its cyber-security performance.

A

XDS  
Blockchain

B

Timeline

Update alternative access pathway

Request Mr.Bob’s document via contact info. provided by META in registry.

Return Mr.Bob document

Figure 5 Augmentation from original framework

# IMPLEMENTATION

This section explains about our implementation to demonstrate the proposing concept.

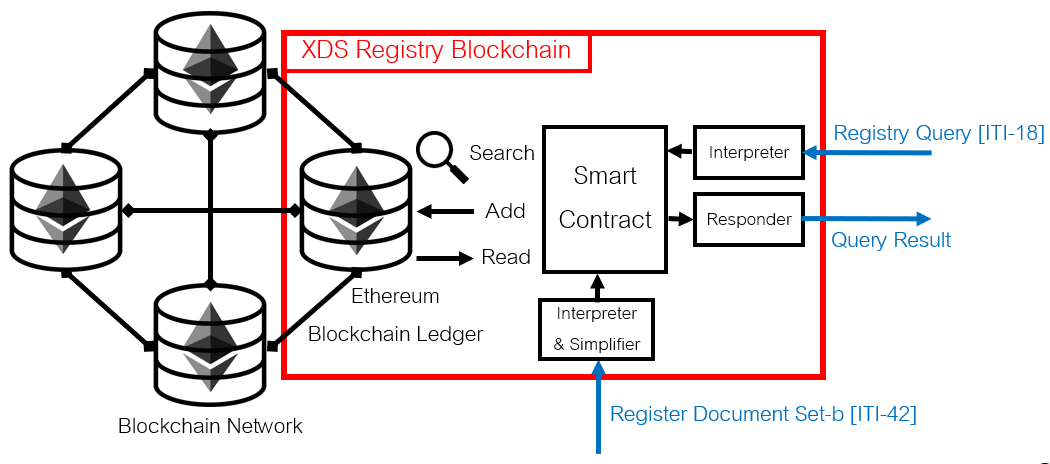
## XDS.b Profile review, requirement gathering, and transaction analysis

 For an adaptation of IHE XDS in this work, we assumed that XDS Domain focuses only on exchanging stable health documents and XDS affinity domain members are using a shared patient identifier. This means if following Figure 1, On-Demand Document Repository Actor and Patient Identity Feed Actor can be excluded from our implementation which reduces the complexity of concept demonstration. At the same time, XDS Document Sources Actor will also be excluded from our scope of interest as it is not directly interacting with our implementation of the Blockchain concept. In this work, we required to substitute the relational database of the XDS Document Registry Actor with the Blockchain ledger. This Blockchain implementation needs to have most of the capabilities that a common relational database could do included adding, query, retrieve, and update. However, insert and delete operation may not be able to achieve due to the limitation of Blockchain which makes it impossible to remove data from its ledger or replace its sequence and the main purpose of implementing IHE XDS with Blockchain is to make it immutable. The Blockchain needs to be able to operate seamlessly with XDS Document Registry Actor. XDS Document Registry Actors in this implementation must have interoperability with XDS Document Repository Actors and XDS Document Consumer Actors while having these actors modified from specification in IHE ITI Framework at least possible. This should allow a simpler adoption process for those organizations with IHE XDS already implemented.

## Acquiring IHE ITI transaction samples

As to test if this implementation can operate with XDS Actors in a common XDS system, we use transaction samples provided by the IHE ITI framework with modified attributes value to evaluate the system. Transaction samples provided by the framework are including ITI-42 Register Document Set-b transaction, ITI-18 Registry Stored Query transaction, and its corresponding response transaction. However these transaction samples have limited capabilities as an example due to much more specification provided in the framework so, there is some transaction need to be defined manually from example and requirement provided in the framework.

Figure 4 Overview of the design to integrating Blockchain with XDS.b Framework



## XDS Document META-data attributes analysis

META-data attributes are those attributes value and elements used to describe its original health document which allows interoperability between each actor in IHE ITI Framework. The attributes mainly compose of attributes that describe originating of the document, information related to event represented by the document, document identifier, information of patient participating the event, information of healthcare personal and facility performing the event, document location, communication protocol in healthcare domain for document interpretation, and document technical information. Having META-data attributes allow XDS Actor to discover and exchange health document from other actor within its affinity domain. In our adaptation of XDS, XDS Document Registry Blockchain must be able to response to query from XDS Document Consumer Actor with specified META-data attributes value as search keyword.

## XDS Document Registry Blockhain process flow

The flow is separated into two parts including document registering and document query. For document registering, XDS Document Repository Actor register document META-data attributes into XDS Document Registry Actor using IHE ITI-42 transaction. XDS Document Registry Actor then interprets the transaction into a programmable object before check if the transaction is ITI-42. Then, the actor proceeds to pass the retrieved object into Blockchain smart-contract and publish it into a Blockchain ledger. For document query, XDS Document Consumer query for document META-data attributes stored within XDS Document Registry Blockchain providing search operation type and some META-data attributes value as search keyword via ITI-18 transaction. XDS Document Registry will check if the transaction is ITI-18 before performing search operation matching specified search type using provided keyword META-data attributes value. The search operation will be performed by consequently call for each registered smart-contracts until all contracts with matched attributes value were found. XDS Document Registry Actor then returns all query result in XML format following specification for ITI-18 responding. Upon receiving the query response, XDS Document Consumer then interprets the transaction and displays the result to the user in a human-understandable format.

## Define Blockchain environment requirement

According to our use case scenario, each Blockchain node will be maintain by hospital or healthcare institution. Each maintainer may have more than one Blockchain node active depend on their usage of XDS Document Registry Actor on actual situation. For this implementation, we declare that each Blockchain node represent one of hospital or healthcare institution participate as XDS Affinity Domain members due to limited computational resource for demonstration. Following the design in chapter IV, it is better to use consensus which require small number of node and require as low as possible resource to maintain.

## Blockchain setup

To directly command the behavior of each Ethereum Blockchain node, we require the "Geth" client which allows the user to issue commands to the node like start-stop mining and start sync Blockchain data with other nodes. For programming smart-contract, Ethereum providing a web-based IDE for Solidity language that can compile and deploy smart-contract to local Ethereum node called “Remix” [38]. To interface our program to Ethereum smart contract, we can use Ethereum API tools which is Web3 [39] as a middle. Web3 allows smart contract control through preferred programming language and transitions logic and variables from the language to Solidity. Then, the Blockchain platform is ready for smart contract design and implementation of the XDS.b profile.

## Choosing consensus and Blockchain components

Consider scenario and Blockchain environment, so we choose to use Practical-Byzantine False Tolerance (PBFT) as consensus for Blockchain. PBFT suit best with permissioned Blockchain with known members. The consensus can maintain Blockchain with small number of validator node. Fortunately, there is Ethereum forked named “Quorum” which allow usage of consensus other than Proof of Work and Proof of Stake. In Quorum, PBFT was modified to suitable with Ethereum and being called “Istanbul-Byzantine False Tolerance (IBFT)”. Quorum provided “7 nodes example” which act as simulator for actual Quorum network with 7 active validator nodes that can be used for demonstration of proposed concept.

## Utilize Quorum

Quorum is a Blockchain platform forked from Ethereum with the goal to expand the usability of Ethereum Blockchain for a wider variety of environments regard consensus and its member nodes. Following our design, Quorum can help reduce complexity in utilizing Ethereum smart-contract under PBFT consensus for the work. Quorum also provides virtual "7-Nodes" environment which comprises seven virtual Blockchain nodes for concept demonstration.

## Define XDS Document Registry Actor

In the implementation of this work, XDS Document Registry actor will be the main actor that will be converted from using common database to use Blockchain ledger to keep associated data. The software program must be able to communicate with XDS Document Repository actor and XDS Document Consumer actor. At the same time, the software will need to act as the middle between XDS system and Blockchain. Then, Blockchain platform is ready for smart contract design and implementation of XDS.b profile.

## Utilize Javascript with NodeJS

As we have seen from HL7 and FHIR, current healthcare information exchanged related standards are majorly web-based protocol. Additionally, development of IT infrastructure to support healthcare operation require the capability to handle a huge amount of transaction in a limited amount of time so, it requires our system implementation to be able to handle multitask properly. With asynchronous nature and compatibility with website integration, Javascript is one of the best choices for our implementation of this work. In this implementation, we adopt the "Node.js" variant of Javascript as it was made to build scalable network applications that handle many connections concurrently. Furthermore, Node.js also providing simple access to community-made node modules which offer a wide variety of useful APIs for software development which may reduce difficulty in our implementation further.

## Utilize Web3JS

As mentioned in F, Web3 also provided a programming API for Javascript called "Web3JS" which allows the Javascript program to interact with Ethereum based   
smart-contract. The API can be accessed using the node module provided via Node.js.

## Implementing Document Registry Smart Contract

Smart-contract was developed to store programming logic or algorithm as blockchain transaction. These smart-contract transactions can be compiled by Ethereum client which will give the result of its script or code (for example, read or return specific value). So, we design smart contract which when executed, it will spawn smart contract that stores given document META-data attributes value within number labeled smart-contract instances which encoded in Blockchain transaction. When these instances were called, it will return the stored metadata attributes value back. Allow the search program to identify the set. At the same time, this allows document registry to store within Ethereum Blockchain. These composed to function as Document Registry Smart Contract.

## Implementing Document Search function over smart-contract

As required in IHE ITI Framework, Document Registry Actor must be able to respond to the query from the Document Consumer by returning the META-data attributes of the registered document matched with the query to the consumer. In a traditional database, this can be done by utilizing a query of a relational (SQL) database. However, for Blockchain, the structure of stored data are different from relational database but similar to NoSQL. That mean, search operation will need to rely on a sequential search algorithm. The program will need to take a look at all published transactions one-by-one from the first until the result was found. Each transaction will require the program to call on smart-contract for reviewing the stored value before comparing it with the specified value used for search. When all of the values called from the smart-contract are matched with the value specified for search, the value called will be marked as a search result which will be returned to XDS Document Consumer Actor via ITI-18 format.

## Interprete XML messages with xml2js module

All actors within IHE XDS Profile communicate with each other using XML message transaction. As we utilize Javascript as main programming language for the implementation, these XML messages need to be interpreted into programming object to allow simpler handling method within the program. Javascript Object Notation (JSON) is a lightweight data-interchange format of programming object which was invented to serve the purpose. It is easy for humans to read and write and easy for machines to parse or generate. That mean, all XML message transactions sent to XDS Document Registry actor program will be converted into JSON. For this implementation, we utilize NodeJS “xml2js” module for the task.

## Implementing IHE ITI-42 transactions interpreter

IHE ITI-42 is XML format transaction used for registering META-data attributes of new document storing in XDS Document Repository actor into XDS Document Registry actor. The transaction specified with header “RegisterDocumentSet-b” and compose of META-data attributes of corresponding document. The content of the attributes varies upon type of document and the event represent by the document. For this implementation, XDS Document Registry actor will open TCP connection to receive the transaction on specified port. After ITI-42 transaction is received, the actor then converts XML message into JSON using xml2js. After that, the program extracts META-data attributes and prepare it for smart-contract.

## XDS Document Registry actor

When ITI-42 was interpreted into JSON, the actor then passes the object into smart-contract. For the implementation, smart-contract was designed to store string value and will return the stored value when called by Geth client. The prepared JSON must be converted into string before entering smart-contract. This is due to limit of Ethereum smart-contract which can cover limit number of programming variable so, we simplify our program to avoid that limit by storing whole JSON in string form as single variable. However, because of Ethereum Blockchain require certain amount of gas to execute smart-contract, the length of the variable may cause error in the process if there was not enough gas supplied. That mean, we need to increase limit amount of gas for executing smart-contract from default value. Although, this change is not affecting this implementation for concept demonstration but, it may affect the network where its member prefers to use actual cryptocurrency like Ether to maintain Blockchain. This may accelerate depletion of currency circulating in the network and severe maintainability of the chain. By these smart-contract design, XDS Document Registry actor can keep META-data attributes of each document by store it as JSON string variable inside Blockchain using one smart-contract per document. At the same time, the actor can perform search operation by sequentially call upon each published smart-contract one-by-one until the result was found or until the last in the case which no matching result. Publishing of smart-contract require gas to execute while calling smart-contract not consuming Blockchain resource.

## Implementing IHE ITI-18 transactions interpreter

Similar with IHE ITI-42 transaction handling, XDS Document Registry actor also wait for ITI-18 on TCP channel. The received transaction will be converted into JSON. The transaction specified with header “QueryResponse” and compose of META-data attributes value input by Document Consumer. These values will be used in search operation which will seek for the smart-contract with matching META-data attribute values. After the result was found, the actor then proceeds to create response XML message following the format provided by IHE ITI Framework.

## XDS Document Consumer actor

Following IHE XDS Profile, XDS Document Consumer actor is where the user specifies search keyword values of META-data attributes for system to query for matching document exist within XDS Affinity Domain. For this implementation, we design that user interface will take a form of command line program that can be run via Windows command prompt or Linux terminal. The program will prompt the user to specify search type, including META-attributes value, and specify the value. The actor then accepts these values to create XML message following ITI-18 format before sending it to local or accessible XDS Document Registry actor to query for matching document and start search operation.

## Performance Evaluation

In this implementation, we evaluate the result concept demonstration by measuring performance of each major process. This will reflect compatibility of the concept to healthcare operation environment which require continuous and huge amount of process at short amount of time.

# Conclusion

## Performance Evaluation Result

In this implementation, we evaluate the result concept demonstration by measuring performance of each major process. This will reflect compatibility of the concept to healthcare operation environment which require continuous and huge amount of process at short amount of time.

## Implementation Source Code

We are providing source code of the implementation at (<https://github.com/semiangel/XDSchain.git>). However, must be noted that this implementation relies on virtual   
nodes provided by Quorum “7 Nodes Example”. Any implementation on additional physical node or separated virtual machine may require additional adjustment on network connection between nodes.

# discussion

This work proposed the idea about implementing IHE XDS.b profile based on Blockchain technology in the goal to allow health document sharing between enterprises while reduce the friction that prevents health information sharing amongst healthcare industry to make it to reality by addressing “trust” issue with Blockchain. And with Blockchain implemented, it also helps increase sustainability of health information network against cyber-attacks. For example, in the case that some hospital may be hit by ransomware and lose access to health documents, this proposed Blockchain concept may assist in retrieving lost documents from other network members who shared the documents.

# References

[1] D. H. Interoperability, “Digital Healthcare Interoperability,” no. October, 2016.

[2] PolicyMedical, “Interoperability in Healthcare: To Have or Not to Have.” https://www.policymedical.com/interoperability-healthcare/ (accessed Sep. 22, 2018).

[3] Carestream Health, “Interoperability : Connecting the Healthcare Enterprise to Deliver Responsive Patient Care,” pp. 1–9, 2015, [Online]. Available: http://www.carestream.com/clinical-collaboration/sites/default/files/WhitePaper\_CCP\_Interoperability\_LTR\_201508\_en\_Web.pdf.

[4] Paige Goodhew, “Why Healthcare Interoperability Matters | Redox.” https://www.redoxengine.com/blog/why-healthcare-interoperability-matters/ (accessed Apr. 27, 2019).

[5] Dr.David Hay, “Why is interoperability so important for healthcare organisations? | Orion Health.” https://orionhealth.com/global/knowledge-hub/blogs/why-is-interoperability-so-important-for-healthcare-organisations/ (accessed Apr. 27, 2019).

[6] Oracle, “Interoperability : A Key to Meaningful Use,” *Solutions*, no. November, 2010, [Online]. Available: http://www.oracle.com/us/industries/healthcare/interoperability-wp-188782.pdf.

[7] Healthcare Information and Management Systems Society, “Definition of Interoperability,” *Himss*, p. 2013, 2013.

[8] HIMSS, “What is Interoperability?” https://www.himss.org/library/interoperability-standards/what-is-interoperability (accessed Apr. 27, 2019).

[9] IHE International Inc, “About IHE.” https://www.ihe.net/about\_ihe/ (accessed Sep. 11, 2018).

[10] “FHIR v4.0.1.” https://www.hl7.org/fhir/ (accessed Oct. 13, 2020).

[11] W. E. Hammond and J. J. Cimino, *Standards in Medical Informatics*, no. December. 2001.

[12] DICOM Library, “About DICOM SOPs.” https://www.dicomlibrary.com/dicom/sop/ (accessed Oct. 22, 2018).

[13] S. Rosslyn, “DICOM PS 3.15 Security and System Management Profiles,” *DICOM Stand.*, 2011.

[14] The Royal College of Radiologists Board of the Faculty of Clinical Radiology, “DICOM and HL7 standards.”

[15] Healthcare IT News, “The biggest healthcare breaches of 2017.” https://www.healthcareitnews.com/slideshow/biggest-healthcare-breaches-2017-so-far?page=1 (accessed Sep. 11, 2018).

[16] HIPAA Journal, “Largest Healthcare Data Breaches of 2018.” https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018/ (accessed Apr. 27, 2019).

[17] Healthcare IT News, “The biggest healthcare data breaches of 2018 (so far).” https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far (accessed Apr. 27, 2019).

[18] “The 10 Biggest Healthcare Data Breaches of 2019, So Far.” https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far (accessed Mar. 04, 2021).

[19] “UPDATE: The 10 Biggest Healthcare Data Breaches of 2020.” https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020 (accessed Mar. 04, 2021).

[20] “Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak | ZDNet.” https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/ (accessed Mar. 04, 2021).

[21] D. Cosset, “The 4 characteristics of a blockchain - DEV Community.” https://dev.to/damcosset/the-4-characteristics-of-a-blockchain-2c55 (accessed Oct. 29, 2018).

[22] Deloitte, “Key Characteristics of the Blockchain,” Accessed: Oct. 29, 2018. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/industries/in-convergence-blockchain-key-characteristics-noexp.pdf.

[23] Data Flair, “6 Major Features Of Blockchain | Why Blockchain is Popular?” https://data-flair.training/blogs/features-of-blockchain/ (accessed Oct. 29, 2018).

[24] Techracer-Medium, “4 Key Features of Blockchain – Techracers – Medium.” https://medium.com/techracers/4-key-features-of-blockchain-5a4aff025d38 (accessed Oct. 29, 2018).

[25] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain Technology Overview (NISTIR-8202),” *Draft NISTIR*, p. 59, 2018, doi: 10.6028/NIST.IR.8202.

[26] henriquegaia, “ethereumbook/07smart-contracts-solidity.asciidoc at develop · ethereumbook/ethereumbook · GitHub.” https://github.com/ethereumbook/ethereumbook/blob/develop/07smart-contracts-solidity.asciidoc#what-is-a-smart-contract (accessed Aug. 23, 2020).

[27] V. Buterin, “A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM.”

[28] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, “A Blockchain-Based Approach to Health Information Exchange Networks,” *Mayo Clin.*, no. 1, p. 10, 2016, doi: 10.1016/j.procs.2015.08.363.

[29] G. Zyskind, O. Nathan, and A. S. Pentland, “Decentralizing privacy: Using Blockchain to Protect Personal Data,” *Proc. - 2015 IEEE Secur. Priv. Work. SPW 2015*, pp. 180–184, 2015, doi: 10.1109/SPW.2015.27.

[30] IHE International Inc, “IHE IT Infrastructure ( ITI ) Technical Framework Volume 1 Integration Profiles,” *Int. J. Healthc. Technol. Manag.*, vol. 1, no. 8.0, pp. 1–177, 2008, doi: 10.1504/IJHTM.2008.017371.

[31] “Blockchain Consensus: A Simple Explanation Anyone Can Understand.” https://blockgeeks.com/guides/blockchain-consensus/ (accessed Oct. 13, 2020).

[32] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, “A review on consensus algorithm of blockchain,” *2017 IEEE Int. Conf. Syst. Man, Cybern. SMC 2017*, vol. 2017-Janua, pp. 2567–2572, 2017, doi: 10.1109/SMC.2017.8123011.

[33] “Proof-of-Work, Explained.” https://cointelegraph.com/explained/proof-of-work-explained (accessed Oct. 13, 2020).

[34] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, “PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain,” *CEUR Workshop Proc.*, vol. 2058, pp. 1–11, 2018.

[35] D. Drescher, *Blockchainbasics*. Apress, Berkeley, CA.

[36] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, no. June, pp. 557–564, 2017, doi: 10.1109/BigDataCongress.2017.85.

[37] K. Sultan, U. Ruhi, and R. Lakhani, *CONCEPTUALIZING BLOCKCHAINS: CHARACTERISTICS & APPLICATIONS*. 2018.

[38] “Remix - Ethereum IDE.” https://remix.ethereum.org/ (accessed Mar. 08, 2021).

[39] “web3.eth.Contract — web3.js 1.0.0 documentation.” https://web3js.readthedocs.io/en/v1.3.4/web3-eth-contract.html (accessed Mar. 08, 2021).