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

*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-b (XDS.b) profile that allows the adopted organizations to share health documents between each others. No specific security implementations were endorsed for XDS.b, 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 affect 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.b

# Introduction

//introduce health record, current problem and motivation

The increasing demand for more secure and high-quality healthcare services, as well as operational efficiency, all have a significant impact on patient care and economic outcomes. Healthcare information sharing and interoperability among healthcare organizations are critical components of enhancing the quality of healthcare services. Patients' health records are scattered across multiple healthcare organizations, which may be due to the fact that various medical services are offered by various providers. Each healthcare provider's methods, processes, and workflow are unique in how they manage healthcare information. This complicates interoperability between health information systems. Sharing health information with trusted third parties who may not adhere to the highest security standards and practices exposes patients, businesses, and organizations to vulnerabilities. The risk-reward ratio associated with sharing patient information between healthcare institutions may be unfavorable if done incorrectly. Additionally, it is difficult for patients to give full permission 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].

//introduce current solution XDS

Therefore, to address these mentioned issues, there are many initiatives [9–14] that are starting to standardize healthcare information technology with the goal of allowing healthcare organizations to be able to exchange patients' information with one another. Amongst them, the Integrating Healthcare Enterprise (IHE) is an initiative that provides a standardized framework that emphasizes enabling interoperability between each unit of healthcare services workflow. To address the issue of health information sharing between multiple organizations, IHE has provided the Cross-Enterprise Document Sharing Profile. The Profile offers a detailed framework for software developers and system architects about how different enterprises share their health documents with each other. The Profile also acts as a guideline, providing essential protocols for system implementers to follow.

//introduce security problem in health record

More than the issue regarding health information sharing between different enterprises, cyber-security threats are also an emerging issue threatening the healthcare domain. Since 1989 [15], hospitals have been hit by ransomware, and it has interrupted medical operations and severely disrupted healthcare services. The number of patient records breached has been increasing every year from 2012 to 2020 [16–20]. Security experts estimated the number of ransomware attacks on healthcare institutes to be close to 1,000 per day in 2015, which is 35% more than the year 2014 [19]. The number even rose to 4,000 attacks on certain days, according to a report published by Symantec in 2016. The case of the Czech hospital hit by a cyberattack during a COVID-19 outbreak [21] demonstrates that failing to secure the integrity and availability of healthcare information causes a significant disruption in the continuity of medical operations. Moreover, as traditional healthcare information infrastructure was separately developed as a centralized system, when one system goes down, all of the connected systems are also affected and become "The Single Point of Failure" (SPOF) [22]. This further synergizes the impact of cyber-incidents on healthcare information systems to be more crucial.

//introduce current security solution i.e. Blockchain

To address the single point of failure problem, the concept of decentralization was introduced. Decentralization eliminates the need for a centralized mediator for one system to operate. That mean even one system amongst the decentralized network went down, the connected system may not be affected and withstand failure. Together with the concept, the blockchain technology was also introduced as a base technology to achieve decentralization. Blockchain technology is one of the solutions to secure healthcare information. The immutable characteristics of blockchain's cryptographic components and consensus mechanism will ensure the integrity of the information, while decentralization of published data will help ensure its availability. [23–26]. Blockchain is generally described as a distributed digital ledger of cryptographically signed transactions grouped into blocks. [27]. Each block is cryptographically associated with the preceding block, making it tamper evident. This is achieved after the transaction validation and after going through a consensus decision amongst nodes on the blockchain network. This endows it with the ability to withstand threats to information integrity and availability.   
At the same time, with consensus as a vital part of the Blockchain, it allows members of the Blockchain network to systematically "trust" each other without the need for mutual trust or physical agreement. Furthermore, because Blockchain is a distributed and decentralized network, each member must share information with one another in a passive manner. Since the introduction of the first blockchain-based cryptocurrency named "Bitcoin", there have been many blockchain platforms and service providers that have entered the industry. One of the major platforms adopted by many kinds of applications is Ethereum. It was the first major platform that introduced the 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 onto the Blockchain, enabling a wide range of applications. [26,27].

//existing solution works + their lacking, shortcoming

As for addressing issues regarding health information sharing between different enterprises, there are concepts of utilizing Blockchain proposed by Mayo Clinic [30] at MIT. Both introduce an effective way to utilize Blockchain technology for information sharing in a healthcare enterprise environment. The work has given a great demonstration of how the decentralization offered by Blockchain can resolve trust issues where each enterprise requires "trust" before beginning to share their information with others. There is also the work proposed by Sudeep Tanwar et.al. [31], which surveyed all the proposed healthcare blockchain concepts and summarizes the situation in the field of research. However, neither solution has explicitly stated how Blockchain can aid in the mitigation of cyber-security threats threatening the integrity and availability of data in the healthcare domain. In this work, we propose a solution that can solve data integrity and availability issues while helping reduce the friction of allowing health document sharing between different enterprises by utilizing Ethereum’s Smart-contract to enable implementation of the IHE XDS.b profile on Blockchain.

//our proposed work

To address the issue of trust to enable cross-enterprise health document sharing while avoiding a single point of failure, we propose applying Blockchain technology to the Cross-Enterprise Document Sharing-b (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 allows for the passive distribution of data to the network via a blockchain-specific protocol without the need for a centralized mediator. Cryptographic chain characteristics establishes 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 or prevent tampering of existing data. Combining Blockchain with XDS.b will significantly reduce data sharing risks, even if 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 everyone to integrate, share, and keep track of their own healthcare information at its best.

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 discussed about the proposed concept in section VI and end with conclusion of this work in section VII.

# RELATED WORK

There are several related works proposed about the concept of implementing Blockchain technology

## A Blockchain-Based Approach to Health Information Exchange Networks

Kevin Peterson et al. [30] 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 concepts about using computational resource within Blockchain network in the more meaningful way contribute to healthcare environment. Additionally, the work also included many suggestions about Blockchain components that may provide more compatibility of the technology for healthcare information environment. However, the work did not mention about how Blockchain technology can be beneficial for health information sharing in term of cybersecurity. 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.

## “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 store metadata about the record ownership, permissions and data integrity representing existing medical records that are kept in 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” [32]. 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. [33]. 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 allows 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.

C. Blockchain-based electronic healthcare record system for healthcare 4.0 applications

Sudeep Tanwar et.al. [31], surveyed proposed healthcare blockchain concepts from 2016 to 2019 which would benefit the healthcare industry by enhancing the capabilities of electronic health records. The work has effectively explained the overall concept of incorporating Blockchain technology into electronic health records that has evolved over time. They also proposed a different approach to implementing Blockchain technology for electronic health records by using IBM Hyperledger fabric as a medium for health information exchange. Similar to MedRec, their concept emphasizes improving access control and audit trail over information exchange between each unit of the healthcare service workflow. The work sets another example of effectively implementing blockchain smartcontracts for the possibility of healthcare blockchain. [31].

# BACKGROUND KNOWLEDGE

Prelude…

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

Modern healthcare operations have large amount of healthcare information flow between multiple systems. Throughout the age, many medical service providers and organizations have developed their own health information systems and databases to increase efficiency of operations 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.

IHE is significant initiative by healthcare professionals, organizations, and industry to enhance the way health information systems in healthcare integrate and share information. It promotes the coordinated use of established standards such as information technology standards, HL7 and DICOM [14] to address specific clinical needs in support of information system integrations and optimal patient care. This helps enable seamless health information exchange that is usable whenever and wherever needed. Health information systems developed in accordance with IHE integrate and exchange information with one another better, are easier to implement, and enable healthcare providers to use information more effectively. An IHE profile provides use of existing standards, specifications, tools, and services for interoperability. It also engages healthcare institutions, 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.

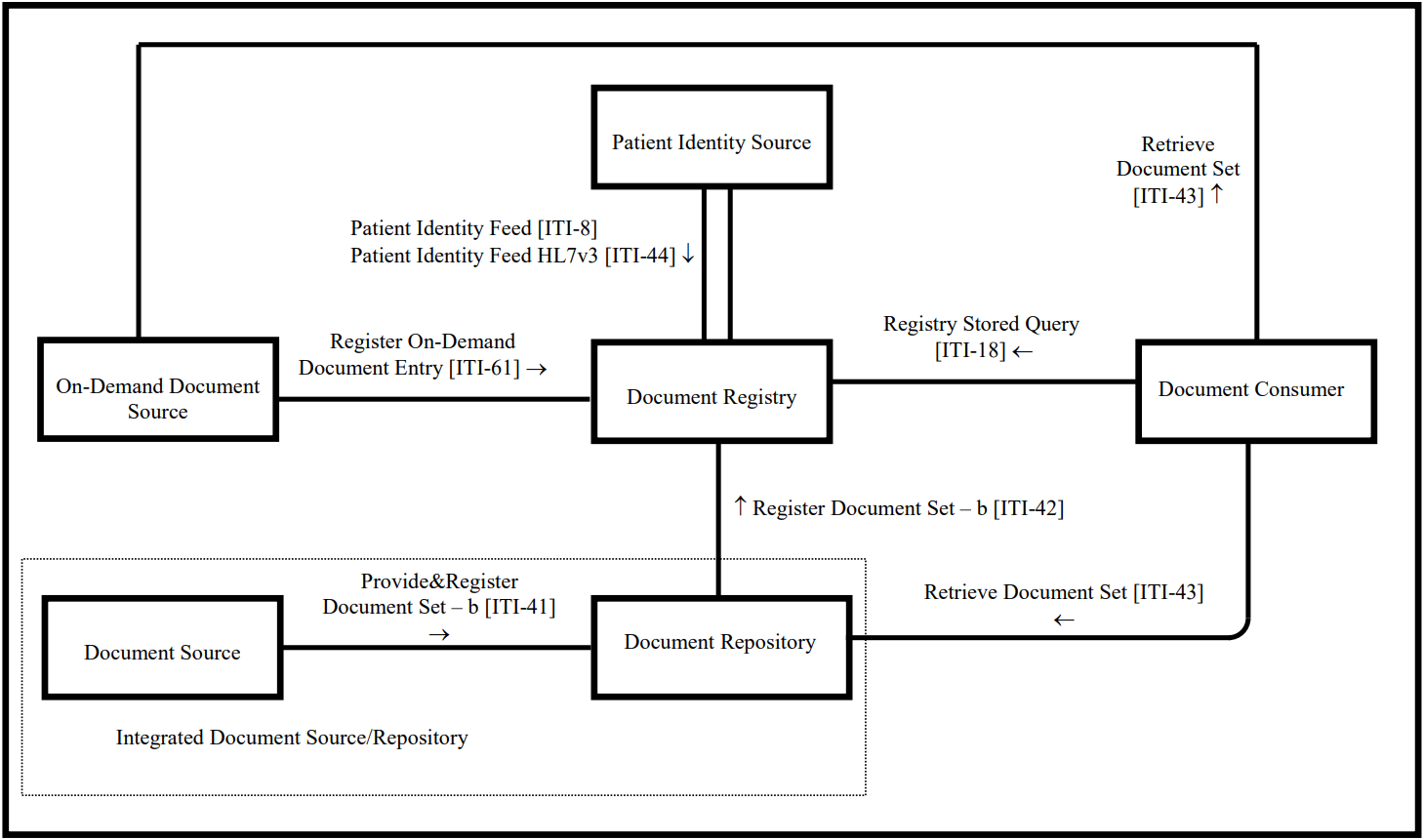


Figure 1 Cross-Enterprise Document Sharing – Set b [34]

Amongst many profiles created by IHE, there is one major profile that serves to improve efficiency of health information sharing between different enterprises called “Cross-Enterprise Document Sharing Profile-b (XDS.b)” [34]. 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 documents available within XDS Affinity Domain and enable interoperability between corresponding software. Document Consumer Actor queries for information of registered documents 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 [27]. 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 represents 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 ensures 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 [35].

According to [27], 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 [36].

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 [37]. 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 [38]. 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 uses voting mechanism which sacrifices 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 [39]. 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.

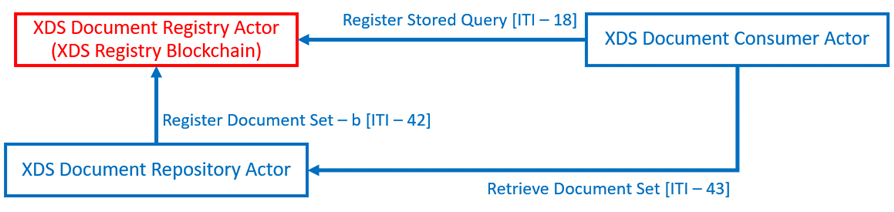
## Ethereum and Smart-Contract

Ethereum [Ref] 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 [24] 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. It starts 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 2 XDS Profile within the scope of interest for this work



## A Use Case Scenario

Mr. Peter Parker was bitten by a strange spider. Mr. Parker then visited hospital A seeking for medical advice. A doctor at hospital A examined the wound and saw no unusual effect on Mr. Parker and dressed the bite wound for him. The encounter event and diagnosis result were recorded within hospital A. Later, during his travel to another city, Mr. Parker felt quite painful from the bite area. He then visited hospital B for further consultation. Without the health information sharing standard implemented between the two hospitals, the doctor at Hospital B could not see the diagnosis result from hospital A. The situation becomes even worse when the health information system of hospital B was hit by ransomware and went down. That means a doctor at Hospital B cannot know that what happened to Mr. Parker. On the other hand, with IHE XDS Blockchain implemented, even hospital B hit by ransomware, a doctor at hospital B can use an alternate machine to access the XDS Blockchain ledger and discover that there is the latest diagnosis result for Mr. Parker available at hospital A. A doctor then gains access to the diagnosis result and able to identify that Mr. Parker was afflicted by unknown genetic mutated symptom caused by the spider bite. Allow the doctor to prevent a further harmful consequence.

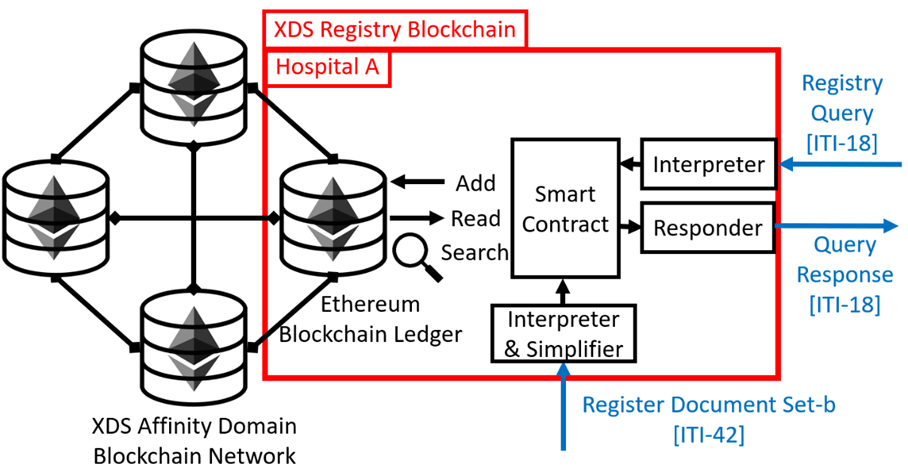
## Conceptual Design

The unique nature of the healthcare information system and its environment emphasizes confidentiality of data that limits full use of Blockchain technology. Patient data cannot be put directly into Blockchain as it will become persistent following Blockchain characteristics while increasing difficulty in ensuring data confidentiality when its replica is distributed all over the network. Instead of risking confidentiality of healthcare data by publishing it directly into the Blockchain network, we propose using IHE XDS.b Document Registry Actor to act as a health document exchange medium for the Blockchain network. The profile is best compatible with Blockchain technology as decentralization will secure the availability of the health information exchange by eliminating the need for the organization that will act as the central hub for the exch iป ange avoiding a single point of failure problem. At the same time, there is no need to publish health documents directly into the distributed network, reduce the risk against the data leakage. Additionally, we further extend the usability of the profile by allowing the organization that has shared health documents from its source to also act as an additional data backup for the original by providing additional access points (URLs) for the document. That means even the source of health document becomes unavailable due to unpredictable circumstances like a cyber-incident (i.e., ransomware threat), the network will still have a chance to access the compromised document via an alternative source available from a shared peer. This extends the benefit of the health document sharing network and encourages the growth of the health document sharing community even further.

## Blockchain Design

Considering the environment of the XDS Affinity domain network, the network is comprised of members who are hospital or health institution that entered the network intending to share their health document and access health document shared from other. Each member entering the network are expected to have been selected by the network and have an agreement with the network to voluntarily share health document from their XDS Document Repository Actor to the network while not exposing information shared within the network to the outside. Following Blockchain Types mentioned in 2.3.2, the network is not suitable with the Public Chain as they are not accepting anyone into the network without pre-selection and a proper agreement. At the same time, they are also not suitable with the Private Chain as the XDS Affinity domain network was designed for scalability and not fixed to any specific organization. That means the XDS Affinity domain network is best suitable with the Permissioned Chain type [Reference?] as it was designed for scalability welcoming more members to join the network over time under the condition that joining members are accepted by the network and have a proper data sharing agreement.

Figure 3 Integrating Blockchain into XDS.b Profile



Meanwhile, following the Blockchain consensus mentioned in 2.3.3.4, the XDS Affinity domain members were not pre-determined to invest a high amount of computational resources for entering the network and were not expected to gain direct profit from participation in maintaining the network. That means the consensus mechanism with computational resources inefficiencies like competition-based and profit-dependence mechanism like randomness-based are not the choice of consensus for the network. Then the remaining majority-based consensus will be the most suitable choice available. The starting point of majority-based consensus will be PBFT as the basis of the type. With the nature of the XDS Affinity domain network which pre-determined the joining member, this should prevent the chance for the bad actor to control the majority and secure Blockchain characteristics for the network consecutively.

## Integrating Blockchain with XDS.b Profile

For the implementation, we assume that the ITI-61 transaction is unessential for the current usage of the work because ?????. The patient identification was assumed to be already standardized amongst all members of the network, eliminates the need for the ITI-44 transaction from consideration. This left the XDS Document Registry Actor Blockchain to only interact with the remaining XDS Document Repository Actor via ITI-42 transaction and XDS Document Consumer Actor via ITI-18 transaction (as shown in Figure 2).

All Blockchain nodes will receive ITI-42 transactions from their local XDS Document Repository Actor as normal XDS Document Registry Actor would do, before transitioning the transaction into Blockchain SmartContract and publish into the Blockchain ledger. Likewise, the health document query via ITI-18 transactions from local XDS Document Consumer will be interpreted and interact with SmartContract consecutively. Note that the XDS Document Consumer Actor will still be required to directly issue ITI-43 transaction to the XDS Document Repository Actor hosting the health document to retrieve it. The SmartContract will act as a medium for each node to perform the task to add data, read data, and search for data within the Blockchain ledger (as shown in Figure 3) allow the Blockchain technology to effectively integrated into the XDS system.

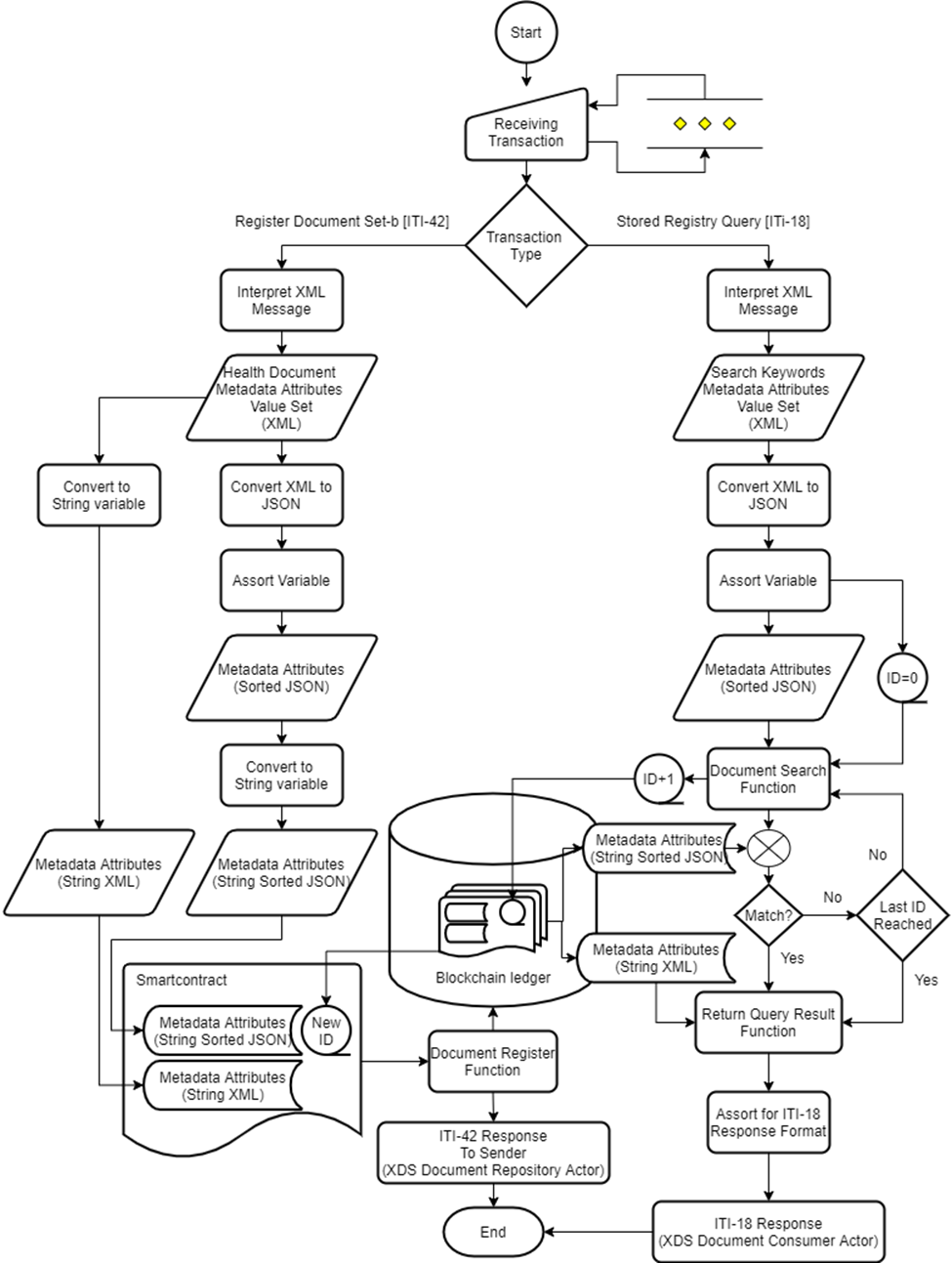


Figure 4 The process flow of XDS Document Registry Actor

## Design Functions of Document Register

This is where XDS Document Registry Actor registers health document metadata set within ITI-42 transaction received from XDS Document Repository into the Blockchain ledger. This function enables sharing of health documents to the XDS Affinity Domain Blockchain network as well as allowing the shared document to be registered as an alternative source. There are two SmartContract functions related. The first function is the document registering function, the function acts as part of the XDS Document Registry Actor to store the value of health document metadata interprets from ITI-42 transaction into the Blockchain ledger. This function acts in a fashion like a programming variable where certain values were assigned to a specific variable for usage within the program, a whole set of metadata value is assigned into single SmartContract function transaction. The function also automatically assigns each set of metadata with an identification number to be used for common understanding amongst the SmartContract to differentiate each set of metadata belong to each health document. The identification number also essential for search operation which would be further explained later. The second function is the checker function which will check for the last identification number assigned to the published set of metadata. This function allows SmartContract to keep track of the identification number previously used and prevent duplication. Each time a new set of metadata entering the Blockchain ledger, the identification number which would be assigned to the metadata set will be additively increased by one from the previous.

Figure 4 depicts the overall process flow of the XDS Document Registry Actor, which performs tasks for both the Document Register and Document Query functions.

# IMPLEMENTATION

This section describes our implementation to demonstrate the implemented concept mentioned previously.

## Blockchain Setup

The application was developed on a laptop Alienware 17 R5, Intel Core i9 with 32 GB of RAM, running on Windows 10 operating system version Home Single Language (20H2) 64-bit, x64-based processor. The resulting code then deploys on the test machine. As most Ethereum-related software is initially designed for Linux OS, so Ubuntu was selected OS for the test machine. The test machine is where all Blockchain-related environment was deployed. A test machine is a virtual machine established within the main machine using Oracle VM VirtualBox. The virtual machine running on Linux Ubuntu (64-bit) version 18.10 with 8 GB RAM and 100 GB storage dynamically shared from the host main machine. Go-Ethereum or "Geth" client is the open sources software engine requiring to operate Ethereum Blockchain within each node. The client allows the user to issue commands to the node like initiate the Blockchain, start-stop mining/validating process for the Blockchain, and activate devp2p protocol to sync Blockchain data with other nodes. The client is available at where??? [40]. Geth can be installed as standalone or included in the installation package of the Ethereum platform variant or other kinds of service interacting with Ethereum Blockchain (i.e., Ethereum Wallet Client). Geth's interface was initially designed to operate on Linux OS and later extend compatibility to other OS via Linux console simulated platform or work under graphic user interface of another client. The Geth client has no specific system requirement as it only is a set of Golang scripts that have no restriction to any system but, as it is mostly integrated within another client, so it requires the machine to be compatible with the main client for installation. In the implementation, the test machine has Geth globally installed by installing Quorum. The client can be launched from anywhere regardless of environment path. Geth can be installed as standalone for ready the machine for working with Ethereum Blockchain using Linux installation from source repository command i.e., “apt-get install ethereum” in Ubuntu. The installation instruction can be located at ??? [41]. All available command lines for Geth can be located at ??? [42]. The most used command is "geth attach <IPC path or Link>" which required for accessing Geth console of each active node. The console is where the user can input the command line to directly control the behavior of each Ethereum Node. Quorum is an Ethereum-forked that allows the Blockchain to adopt a consensus mechanism other than PoW and PoS which default to Ethereum Blockchain. Quorum's source code and installation package can be accessed at ??? [43]. The installation method for the latest stable release is located at ??? [44]. The platform was designed to specifically operate with a Linux-based interface and can be compatible with non-Linux OS with the aid of third party software as a medium. Other than that, the platform has no specific system requirement for installation. However, from the test during the implementation, it is recommended that the machine running Quorum should have more than 6 GB of available RAM. Otherwise, there will be a performance issue that occurred during the run. In this implementation, as the test machine running on Ubuntu 18.10, there is no other 3rd party software required to operate Quorum. The Geth client was included in the Quorum installation package, which means a developer can immediately start their Quorum Blockchain development right after the installation.

Other than the Blockchain platform, Quorum also offers the "7-Nodes Example" for developers to locally deploy in their machine to test the functionaorlity and performance of Smartcontract during the development. The source code can be cloned directly from its repository available in Github [45]. The "7-Nodes" will simulate seven Blockchain nodes in the host machine in a similar fashion to a virtual machine using the required library called "Tessera" [46] and "Constellation" [47] included in the package as a running engine. The source code can be initiated, activated, and simultaneously controlled using the control script provided within the example. Each node can be accessed using the Geth client. For the implementation, the control script(s)??? provided within the example was further modified to be compatible with our usage. The Blockchain initiation script was modified to be able to re-initiate the entire Blockchain by deleting the existing chain and replace with the empty one. This allows reset of published Blockchain during the development. The transaction publishing script was modified to run other specific code developed for XDS Document Registry Actor and its SmartContract allows testing and running of XDS Document registry-related code on the 7-Nodes. It must be noted that transaction-related scripts only operate on specified single nodes amongst the seven, not the entire set of the seven nodes. That means the activity of each node is independent. All initial configuration instructions are available at ??? [48]. Primarily, it is required to configure the genesis Block for the Blockchain ledger and issue the initiation command using the script provided. Each script is specific for each consensus mechanism. In this implementation, we only use the script "istanbul-init.sh" (execute using Linux Bash syntax) to initiate the genesis Block for the Blockchain ledger as we going to use IBFT as its consensus mechanism. The script will generate "istanbul-genesis.json" file as a configuration script for the genesis block. Then the activation of the IBFT Blockchain can be done using "istanbul-start.sh" script which will start the activation of all seven nodes and bring the 7-Nodes Blockchain network to become alive. It must be noted that this activation process may take several minutes.

For this implementation, we further created a script to reduce the complexity of the initiation and activation process of 7-Nodes Blockchain. The script "rebirth.sh" will delete all data of an existing set of 7-Nodes Blockchain and initiate a new genesis file to simplify the reset of the Blockchain during the development of the implementation. The script "runmy7nodes.sh" will issue the whole command line required for activating the 7-Nodes Blockchain, simplify the Blockchain activation process. These scripts will help reduce the complexity of command-line manipulation during the implementation.

For SmartContract programming, Ethereum provides a web-based IDE for Solidity language that can compile, test, and deploy smart-contract to specific Ethereum node called “Remix” [49]. In the implementation, Remix was accessed using Google Chrome from the main machine and the session was saved locally using Remix client to avoid unexpected issues on the Solidity code. Each SmartContract is validated, and test deployed within the IDE before actual implementation on the test machine. The SmartContract ready for implementation will be compiled using the Solidity compiler provided by Remix community-based plugin. Each compiled solidity code gives ABI code and Binary code which will be used on Web3js code to interact with the Blockchain SmartContract. After successfully compiled the Solidity SmartContract code, the ABI code and Byte code will be automatically generated by the IDE. These codes can be copied and passed into Web3js code by assigning a variable to store the code as its value. Noted that Byte code defines the behavior of the SmartContract and only required on the first deployment of the SmartContract which required only once in this implementation, while ABI code defines interface for communicating with the SmartContract and always required every time the native program communicate with SmartContract.

Before begin registering health documents metadata into Blockchain SmartContract, the SmartContract must be first deployed to act as a contract format for the entire Blockchain ledger for the implementation. The Web3js script that simply deploys the SmartContract into the Blockchain ledger. It required both the Byte code and ABI code received from the Solidity compiler to be completed. Once the SmartContract is deployed, any later communication with SmartContract will only need ABI code to act as an interface for the communication. This SmartContract deployment process only required once at the initiation of the Blockchain ledger and no longer needs to be performed ever again for the rest of the Blockchain ledger life cycle.

For the coding process of all non-Blockchain native Javascript programs, the coding environment must be provided essential coding components. In this implementation, we use NodeJS as a compiler and coding environment for all Javascript programs. NodeJS is available at ??? [50]. The essential coding components node module can be installed using Node Package Manager (NPM) which comes together with NodeJS [51]. The coding of program for native side of XDS Actor requires node module name "Web3" (Web3js) [52], "xml2js" [53], "fs" [54], "net" [55], "util" [56], "moment" [57], and "cryptr" [58] which can be installed using the command-line.

## Implementing XDS Actors for XDS Blockchain

 As we have seen from HL7 and FHIR, current healthcare information exchanged related standards are mostly web-based protocol. Additionally, development of IT infrastructure to support healthcare operation requires 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. 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. JSON (Javascript Object Notation) is a lightweight data-exchange format for programming objects that was created specifically for this purpose. It is simple to read and write for humans, and it is simple to parse or generate for machines. That means 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. To connect our program to Ethereum smart contract, we can use Ethereum API tools which is Web3 [59] as a middle. Web3 allows smart contract control through preferred programming language and transitions logic and variables from the language to Solidity. Web3 provides 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.

XML code of Registry Document Set-b [ITI-42] transaction sample composing of two main sections. The first section labeled with “lcm:SubmitObjectRequest” is where XML schematic information are located and the label also act as marker which tell interpreter program to recognize it as ITI-42 transaction. The second section starts from label “rim:RegistryObjectList” following with “rim:ExtrinsicObject” contains all information regarding corresponding health document. This section is where all Metadata attributes of the document are located. If the Document Registry Actor successfully received the transaction, they must return response. The response transaction included only XML schematic information, message UUID number, and status type “successful”. This response will let the Repository finish its process and end messaging attempt. For document registering, XDS Document Repository Actor register document Metadata 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.

XML code of RegistryStoredQueryRequest [ITI-18] transaction sample composes of three main sections. The first section labeled “query:AdhocQueryRequest” is where XML schematic information are located and the label also act as marker which tell interpreter program to recognize it as ITI-18 transaction. The second section labeled “query:ResponseOption” mark the expected format of query result that will return to Document Consumer. The third section starts from label “rim:AdhocQuery” contain all search keywords issued by Document Consumer. These search keywords are selected Metadata attributes and its value. When Document Registry Actor received the transaction, they will use search keyword provided to search for registry with matched Metadata attribute values. Then it returns the result to Document Consumer Actor as response transaction. With header labeled “query:AdhocQueryResponse”, the transaction contains search result depend on query type specified in ITI-18 transaction. If the query expected for “LeafClass” as result, the response would return Metadata attributes of all matched result in detailed. Otherwise, if the query expected for “ObjectList”, the response would return object reference number of all matched results. These two types of response specifically selected depend on search behavior of Document Consumer Actor’s user. The query which specified “LeafClass” as its search result must provide keyword which unique to its corresponding document, such as document unique ID or object reference UUID. At the same time, “ObjectList” are used to search for wide range of document with generic search keyword and value where discovery of document existent is the main goal.

For document query, XDS Document Consumer query for document Metadata attributes stored within XDS Document Registry Blockchain providing search operation type and some Metadata 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 Metadata 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. Following IHE XDS Profile, XDS Document Consumer actor is where the user specifies search keyword values of Metadata attributes for the system to query for matching document exist within XDS Affinity Domain. For this implementation, we design that the user interface will take the form of a 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 an XML message following ITI-18 format before sending it to a local or accessible XDS Document Registry actor to query for matching document and start search operation. The command-line interface of XDS Document Consumer begins with prompt the user to input registry query types or choose to quit the program. The user will need to specify digit numbers corresponding to the choice. Then, the user will be prompted to input essential metadata attributes required for the query type (i.e., FindDocuments will require attributes included DocumentEntryPatientId and DocumentEntryStatus) before prompt to input other metadata attributes as optional depending on the information the user known. When there are no more metadata attribute values to add, the user can choose to start a query for the document. The XDS Document Consumer Actor program will then accept the input and assort it into the ITI-18 transaction before sending it to XDS Document Registry Actor. After the query has been sent, the XDS Document Consumer will wait for the response from XDS Document Registry Actor. When the response is received, the XDS Document Consumer then shows the metadata attributes the value of the query result in the terminal or just terminates the program if there is no matched result registered.

The XDS Document Registry Actor program must be able to communicate with the simulated XDS Document Repository actor and XDS Document Consumer actor. At the same time, the software will need to act as the middleware between the local XDS system and the Blockchain ledger. The Actor will wait until receiving the XML message transaction and react differently to ITI-42 and ITI-18 transactions. Unlike the XDS Document Repository Actor and XDS Document Consumer Actor, the XDS Document Registry was made to act as the medium between the native system and the Blockchain SmartContract. This section will break down the component of the XDS Document Registry Actor in a pattern different from the rest where it separated by its main function interacting with health document metadata which included Document Registering and Document Search. Each section will break down into JavaScript native program part and SmartContract part. For this implementation, the XDS Document Registry Actor will open a TCP connection to receive the transaction on a specified port. Upon receiving the ITI-42 transaction, the Actor then converts the XML message into JSON using xml2js. When ITI-42 was interpreted into JSON, the actor then assorts the object and sorts it into the SmartContract compatible format.

In the implementation, SmartContract was designed to store string values and will return the stored value when called by the corresponding SmartContract function. The prepared JSON must be converted into a string variable before entering SmartContract. This is due to the limit of the Ethereum SmartContract which can cover a limited number of programming variables so, we simplify our program to avoid that limit by storing the whole JSON in string form as a single variable. Because the Ethereum Blockchain requires a particular amount of gas to run the SmartContract, the length of the variable could produce an error if there isn't enough gas available. That means, we need to increase the limit amount of gas for executing SmartContract from the default value. Although this change may not affect the implementation, it may affect the network where its member prefers to use actual cryptocurrency like Ether to maintain Blockchain where an increase in required gas may accelerate the depletion of currency circulating in the network and severely reduce the maintainability of the Blockchain. By the SmartContract design, XDS Document Registry actors can keep Metadata attributes of each document by storing them as JSON string variable inside Blockchain using one SmartContract per document. At the same time, the actor can perform search operation by sequentially call upon each published SmartContract one-by-one until the result was found or until the last in the case which no matching result. It must be noted that publishing of SmartContract always requires gas to execute the task while calling for the variable value stored in the SmartContract is not consuming any Blockchain resource. It must be noted that at the beginning of the XDS Blockchain network, the base SmartContract must be initially deployed into the Blockchain to allow further registration of health documents for the rest of the Blockchain ledger.

Like IHE ITI-42 transaction handling, the XDS Document Registry actors also wait for ITI-18 on the TCP channel. The received transaction will be converted into JSON while matching UUID with its corresponding metadata attributes. The transaction is specified with the header “QueryResponse” and compose of Metadata attributes value input by Document Consumer. These values will be used in search operation which will seek for the SmartContract with matching metadata attribute values. After the result was found, the actor then proceeds to create a response XML message following the ITI-18 format.

Like the Document Register function, the XDS Document Registry Actor must be able to respond to the Document Search query from the Document Consumer by returning the metadata 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 is different from relational databases but like NoSQL. That means search operation will need to rely on a sequential search algorithm. The program will need to 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 SmartContract 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.

## Implementation Result

The environment of the test machine is running on Linux Ubuntu (64-bit) version 18.10 with 8 GB RAM and 100 GB storage dynamically shared from the host machine.

The Blockchain network environment for the implementation will be demonstrated using the 7-Nodes Example Blockchain. That means there will be seven IBFT Blockchain nodes simulated within the environment of the test machine. The test sample will be monitored from node number one (which would later refer as “1st Node”). To indicate that the implementation has the compatibility to operate with XDS Actors in a common XDS system, we created transaction samples based on the example provided by the IHE ITI framework. 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, there is much more specification provided in the framework that far exceeds the element provided within the example. There may consist of an element that differs from the transaction used in the actual system which may cause an error and need further adjustment in the actual deployment. The main group of XDS Actors in the implementation are XDS Document Registry Actor, XDS Document Repository Actor, and XDS Document Consumer Actor. All files corresponding to the implementation must be included within the directory that contains the 7-Node Examples. The XDS Document Registry Actor is the actor that acts as the medium between the XDS system and the Blockchain network. At the same time, the main function and process triggered in the implementation including Document Register and Document Search (Document Query) are centered around the XDS Document Registry. The XDS Document Registry will always active and standby for incoming transactions.

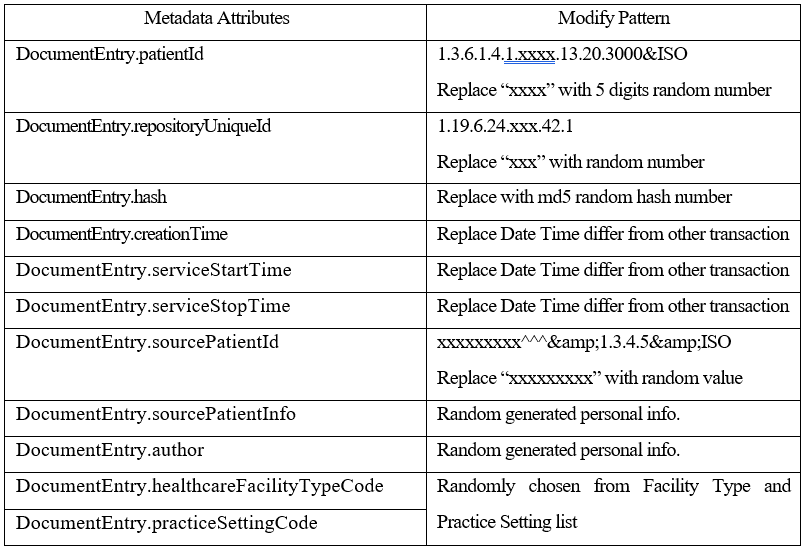


Table 1 Modified metadata attributes in each sample transaction

The XDS Document Repository Actor is the actor that triggers the Document Register function registering new health document metadata attributes set into the Blockchain ledger. The Document Register function is triggered once the XDS Document Repository Actor program was called to register new health document metadata set into the XDS Affinity Domain network. The XDS Document Registry Actor then received the Document Register transaction and proceeds to broadcast the transaction into the Blockchain network publishing the transaction into the Blockchain ledger through a Block validation process. After the transaction was successfully published into the Blockchain ledger, the XDS Document Registry Actor response back to the Document Repository Actor to report that the process was completed which terminating the XDS Document Repository Actor program.

The XDS Document Consumer Actor is the actor that triggers the Document Query function receiving user input search keyword values and asks the XDS Document Registry Actor to search for an existing registered document with the matching metadata attributes value as specified in the search keywords. Once called, the XDS Document Consumer Actor program will prompt the user for document query type then prompt for essential search keyword values and followed by the addition of optional search keyword values. After all search keyword values from the user were set, the XDS Document Consumer Actor program then proceeds to assort the input into the ITI-18 transaction format and send it to the XDS Document Registry Actor. Upon receiving the transaction, the XDS Document Registry Actor program then uses the provided search keywords to search the Blockchain ledger for the metadata set with a matching value. Whether the matching result was found or not, after searching on all registered metadata set, the XDS Document Registry Actor then response search result to the XDS Document Consumer Actor. The XDS Document Consumer Actor then interprets the response and displays the search result to the user.

# evaluation

 The goal of the evaluation is to test the functionalities and the performance of the implemented system. This includes the Document Register function and Document Query function. The evaluation will indicate the compatibility of the implemented system to an actual healthcare operation environment. The implemented system should be able to sustain a huge amount of data that continuously flows through the system without a failure. Each setup will be tested with the mockup transactions and measure the processing time required for the system to complete the specific process. There are ten transactions created for the experiment as test samples. In each transaction have its metadata attributes modified varied in each transaction for the test as shown in Table 1. Each transaction will have about the same file size but different metadata attributes values to prove functionalities of the Document Query function. All experiments will be tested with these transaction samples resulting as 10 times test for each setup ("transaction number #n" will be referred to as "Document#n").

## Functionalities Test

 The main functions of the implemented system are Document Register and Document Query. So, this setup will test the functionalities of each function under the normal circumstance where there are seven active Blockchain nodes and there is one node performing the task. The criteria to check if the Document Register function correctly is the registered document must be discoverable within the Blockchain ledger when its SmartContract was called. This SmartContract must return metadata attribute values of its corresponding document when it was called by the system. The XDS Document Registry Actor signal that it successfully published the metadata attributes set into the Blockchain ledger using SmartContract. When the published SmartContract was called, it returns the value of metadata attributes set. That means the metadata attributes set of Document01 is now live on the Blockchain ledger. This proves that the Document Register is functions correctly.

The criteria to check if the Document Register function correctly is when users input corrected search keywords that match one of the documents registered within the Blockchain ledger, the XDS Document Registry actor must be able to find the matching document and return the search result to the XDS Document Consumer Actor to display it to the user correctly. The XDS Document Consumer user interface that prompts the user to input search keywords matching the document, they are seeking and also show the list of search keywords that match with the Document01. The XDS Document Registry Actor received the query from the XDS Document Consumer Actor and initiate search program. When the XDS Document Consumer found the matching document as the search keywords provided, the XDS Document Registry Actor then returns the search result to the XDS Document Consumer Actor. After the XDS Document Consumer Actor received the search result returned from the XDS Document Registry Actor and display the result to the user. In this case, the result show metadata attributes set for the Document01 correctly. This proves that the Document Query is functioning correctly.

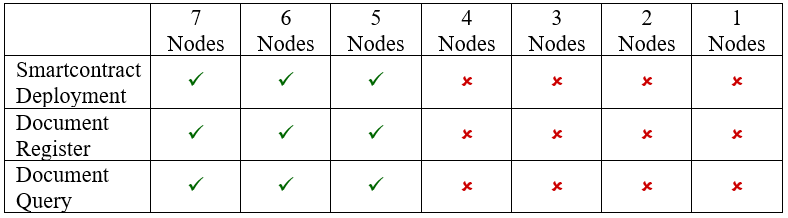


Table 2 Functionalities experiment result

On the hypothesis that a changed number of active nodes may cause a change in the functionalities of the XDS Blockchain, to test the functionalities, the experiment performs by varying the number of nodes and test if the system could perform any function. Start from the setup with seven active nodes as the reference, followed by six, five, four, three, two, and one active node for the variation. To create a situation where there are fewer than seven active nodes, the 7-Nodes Example configuration must be modified to meet the situation. In Quorum 7-Nodes Example, the number of active nodes was defined in the "permissioned-nodes.json" file. Each active node represents by its "enode" identifier number together with its communicating TCP port number. The node will become inactive if its enode number was excluded from the file. That means, in each setup for a specific number of nodes, enode number of inactive nodes must be excluded from the file before initiate the 7-Nodes Blockchain network. At the same time, the "numNodes" variable value in the "istanbul-init.sh" file must be set to the specific number of active nodes (i.e., numNodes = 6 for six active nodes) to declare that there will be file directory prepared for the specified number of nodes at the initiation of the 7-Node Blockchain network. After the configuration was modified, the 7-Nodes Example will automatically generate Blockchain nodes to meet with the specified number upon the initiation of the Blockchain ledger. That means every time the configuration file was modified for a new setup, the Blockchain network must be reset and re-initiated to ensure that there is no conflict with another setup which could affect the accuracy of the experiment result.

Table 2 shows that the system result from the implementation can function normally with 7, 6, and 5 active nodes. The system stops functioning when there are active nodes lesser than 5. After looking into the root cause of the result, it is turn out that the 7-Nodes Example cannot resolve the Block validation process cycle in a situation with fewer than 5 active nodes. When investigate the log, it shows that the Block validation process cycle which would repeat continuously and endlessly simply stopped at the first Block and there is no further upcoming process appeared in the log or none of any error notification appeared. Noteworthy, this is not even related to the condition of IBFT consensus where it requires at least two-third of all nodes to vote for the same Block version to complete the validation process. The system should be able to operate normally without error even there are fewer than five active nodes when all active nodes agreeing on the same Block version and there is no "bad actor node" present in the system to propose a falsified Block version that interrupts the vote. We think that a possible reason could be that the 7-Nodes example may not be developed for the situation with 4,3,2, or 1 active node as it was only built to aid Smartcontract developers to easily deploy and test their SmartContract in the proper 7 active nodes simulated environment closely similar to the actual Blockchain network.

It also must be noted that it is possible for the case that contains an even number of nodes may cause failure in Block validation attempt due to the majority of Block approval from nodes not meet the least requirement of two-third of all nodes in the network. For example, if ten nodes are participating, five nodes proposed Block named 'ABC' while another five nodes proposed Block named 'CBA'. This example will result in failed Block validation attempt. If this happened, the network was expected to try another attempt until the majority meet the least requirement of two-third and all the remaining transactions were successfully added into the valid Block and published into the Blockchain ledger. However, the evaluation of the implementation will not cover the case due to complications in creating the “bad actor” node. We assume that the feature was not directly included with Ethereum, Quorum, or its 7-Nodes Example as it was not created for a malicious purpose so, it is too difficult for us to create the situation that half of the participate nodes attempt to propose falsified Block for the evaluation.

## Performance Test

 On the hypothesis that a changed number of active nodes or change in the amount of XDS transactions entering the system may cause a change in the performance of the XDS Blockchain, the performance test will be performed by triggering the Document Register function and/or the Document Query function depends on the setup. The prepared transaction samples will be tested on the setup with a specific number of nodes then measure the time the system took to complete the process. Additionally, to increase the accuracy of experiment results and reduce the effect from other factors outside the consideration, the experiment will be repeated ten times on each transaction sample. The final performance result of each transaction will be derived from the average values of these ten times repeated.

Test if the number of transactions would cause a change in performance of the XDS Document Registry to perform the Document Register function. This setup is performed by trigger the XDS Document Repository Actor to start the Document Register function which will send the ITI-42 transaction containing metadata attributes set of the selected document (Doc01 - Doc10) to the XDS Document Registry Actor. The processing time the XDS Document Registry took to complete the process publishing the metadata attributes set into the Blockchain ledger will be measured for the experiment result. The "Single Node" line was the averaged processing time monitored at the 1st Node performing the Document Register function when there is only one node performing the function. The "All Nodes" line was the average processing time monitored at the 1st Node performing the Document Register function when all active nodes performed the function within the same time. Both setups measure the processing time the node used to complete the Document Register function since the moment it received the ITI-42 transaction from the XDS Document Repository actor. Figure 5 shows that when all nodes perform the Document Register function at the same time, it took a longer time to complete the function when compared to the situation when there is only a single node perform the Document Register function. The raw results can be further inspected in Appendix Section C. Evidently, the nature of the 7-Nodes Example which its Blockchain nodes need to share processing units of the same host machine could be the main factor affecting the performance. The more processing threads executed together at once mean the more processor resource of the host machine divided for each thread. So, the shared processing unit environment may be affecting the performance of each node resulting in a difference in performance as shown in Figure 5.

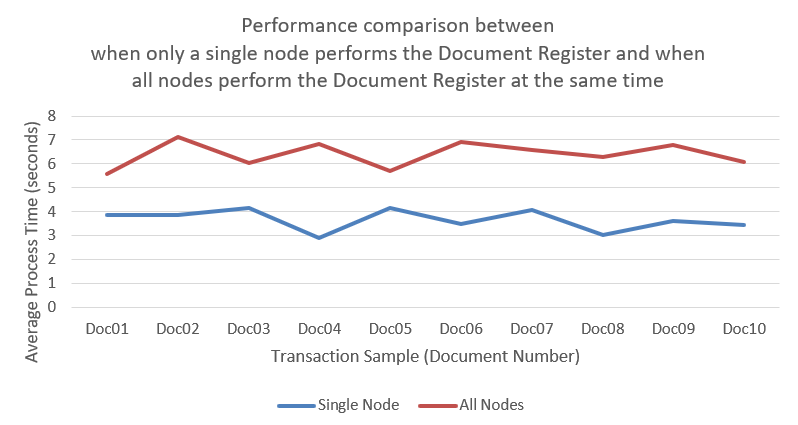


Figure 5 Performance comparison of the system performing the Document Register function between when performed by only a single node and

Test if the number of search keywords would cause a change in performance of Document Query function. This setup is performed by trigger the XDS Document Consumer Actor to start the Document Query function which prompts for input from the user. The user then selected for “FindDocument” query type and inputs metadata attributes values of each transaction sample (Doc01 – Doc10) into the program. The program then proceeds to query for the matching metadata set registered in the Blockchain ledger from the XDS Document Registry Actor in the 1st Node (only one active node received the query). The processing time since the moment the XDS Document Consumer Actor sent the ITI-18 transaction to the XDS Document Registry Actor until the XDS Document Consumer received the search result from the XDS Document Registry will be measured for the experiment result. The "minimum" search keywords will include only two attribute values while the "maximum" search keywords will include fifteen attribute values. The setup for “Single Node” and “All Nodes” is like the first case. The Document Query with the "FindDocument" query type performed by a single node using minimum keywords took an average process time of 285.2455158 milliseconds to complete the function. FindDocument with maximum keywords took an average process time of 287.7405654 milliseconds to complete the function. Performed by all active nodes, minimum keywords took an average process time of 754.1227332 milliseconds to complete the function while maximum keywords took an average process time of 767.9703297 milliseconds to complete the function. Figure 6 and Figure 7 show no significant difference between the Document Query with maximum search keywords compared to the Document Query with minimum search keywords. That means the amount of search keywords input is not affecting the performance of the Document Query function. A full version of the experiment result can be further inspected in the Appendix section. The Document Query function program only used provided search keywords to search for the matching transaction registered in the Blockchain ledger. A greater number of search keywords may take a little more process to finish the search, but the change will not add more significant processing time to the whole process which was expected not to affect the performance of the system.

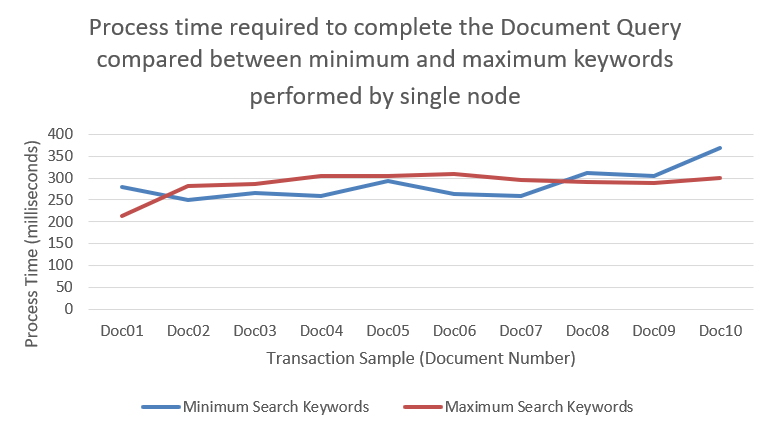


Figure 6 Processing time to complete Document Query   
compared between minimum keywords and maximum keywords performed by single node

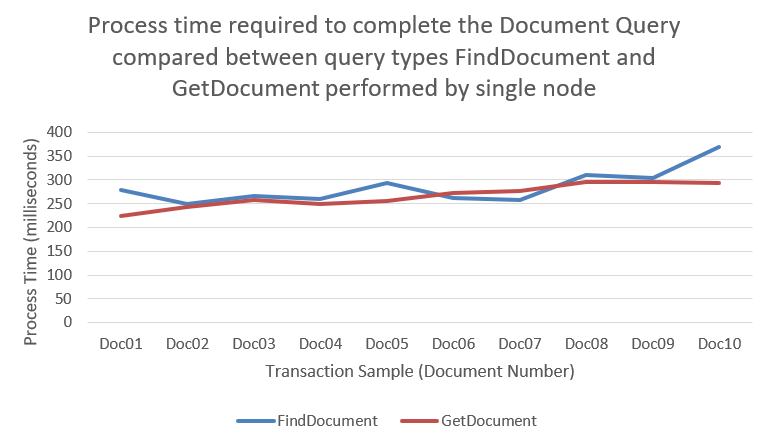


Figure 8 Processing time to complete Document Query  
compared between FindDocument and GetDocument   
performed by single node

Test if different query types would cause a change in performance of Document Query function. This setup is performed by trigger the XDS Document Consumer Actor to start the Document Query function which prompts for input from the user. The user then selected for query type and inputs metadata attributes values of each transaction sample (Doc01 – Doc10) into the program. The program then proceeds to query for the matching metadata set registered in the Blockchain ledger from the XDS Document Registry Actor in the 1st Node (only one active node received the query). The processing time since the moment the XDS Document Consumer Actor sent the ITI-18 transaction to the XDS Document Registry Actor until the XDS Document Consumer received the search result from the XDS Document Registry will be measured for the experiment result. The test begins with the "FindDocument" query type with minimum keywords before the "GetDocument" query type with required keyword (1 keyword). The result then compares the performance of each query type. The setup for “Single Node” and “All Nodes” situation is like Section 4.4.2.1. The Document Query with the "FindDocument" query type performed by a single node using minimum keywords took an average process time of 285.2455158 milliseconds to complete the function. The "GetDocument" took an average process time of 266.3474373 milliseconds to complete the function. Performed by all active nodes, the "FindDocument" took an average process time of 754.1227332 milliseconds to complete the function while the "GetDocument" took an average process time of 765.7761302 milliseconds to complete the function. Figure 8 and Figure 9 show no significant difference between the Document Query with the "FindDocument" query type compared to the Document Query with the "GetDocument" query type. That means the query type is not affecting the performance of the Document Query function. A full version of the experiment result can be further inspected in the Appendix section. The different query types only change the end content of the search result while remain operates on the same base algorithm, so the change will not add more significant processing time to the whole process which was expected not to affect the performance of the system.

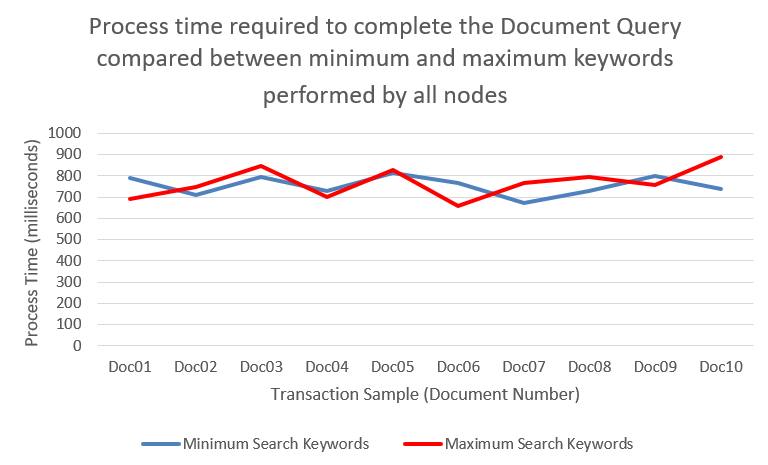


Figure 7 Processing time to complete Document Query   
compared between minimum keywords and maximum keywords   
performed by all nodes

Test if the number of transactions would cause a change in performance of Document Query function. This setup compares all graphs resulting from all cases above to show the overall difference between the case when there is only one single node (1st Node) perform the Document Query function and when all active nodes perform the Document Query function (inspect process time from 1st Node). Figure 10 shows a significant difference between the setup when the Document Query function is performed by a single node and the setup when the Document Query function is performed by all active nodes. When transactions are entering all nodes at the same time, the system took a significantly longer time to complete the Document Query function when compared to the processing time when there is only one transaction from a single node performing the function. That means the number of transactions is affecting the performance of the Document Query function. This could be the effect from the 7-Nodes Example which its Blockchain nodes need to share processing units of the same host machine. This may be the main factor affecting the performance when all nodes need to perform the Document Query function at once at the same time. So, the shared processing unit environment may be affecting the performance of each node resulting in a difference in performance as shown in Figure 10.

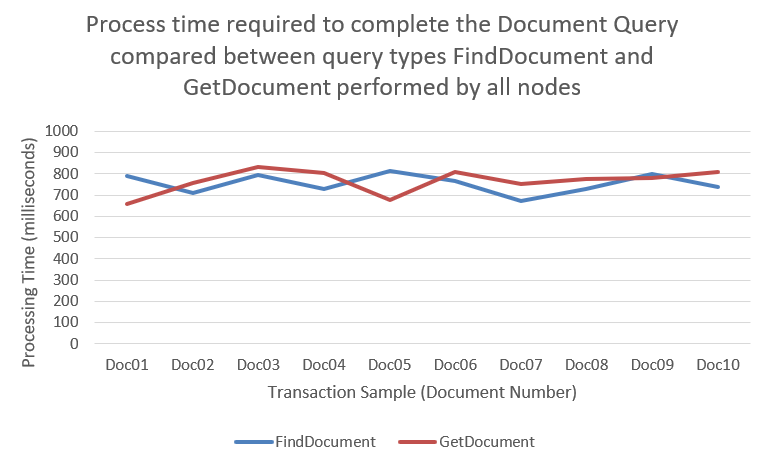


Figure 9 Processing time to complete Document Query compared between FindDocument and GetDocument performed by all nodes

# discussion

Amongst many metadata attributes, there are attributes that value can expose patients' confidential information into the Blockchain network. The attribute "sourcePatientInfo", for example, directly contains personal information for patients whose medical record the document is associated with. This attribute can contain multiple values such as patient name and address. So, in the actual adoption of the proposed concept, these metadata attributes values must be anonymized before entering the Blockchain ledger. This can be done by replacing the value with its hash counterpart when the attributes entering the Blockchain ledger via the Document Register function. At the same time, when the attributes were required for the search operation as search keywords input, the XDS Document Consumer will only need to hash the input value and use the hash to allow the XDS Document Registry actor to search for the matching hash value registered within the Document Registry Blockchain. This allows the concept to maintain confidentiality of patients' data while preserving the functionalities of the concept. During the study on the IHE Profiles standard, we found that the complexity of the IHE standard gave difficulty for interpretation. There are a lot of components including transaction formats, data structures, and specific protocols that are specifically designed for each IHE Profile that published separately in different volumes of IHE Framework documents. Some part of the document was deprecated or obsoleted in the present. There are a limited number of transaction samples available from the framework which makes it difficult for a beginner to develop a system that fully complies with the standard. These make the standard implementation the most time-consuming process. For Ethereum, the usage of SmartContract was limited by its gas requirement. Every task performed by SmartContract requires gas which represents the computational power of the network to perform. That means there will be more factors for the platform to be addressed before the actual adoption. We suggest that the adopted network must be able to provide enough amount of gas or disregard the component from the consideration by integrating it into the common agreement amongst the networks.

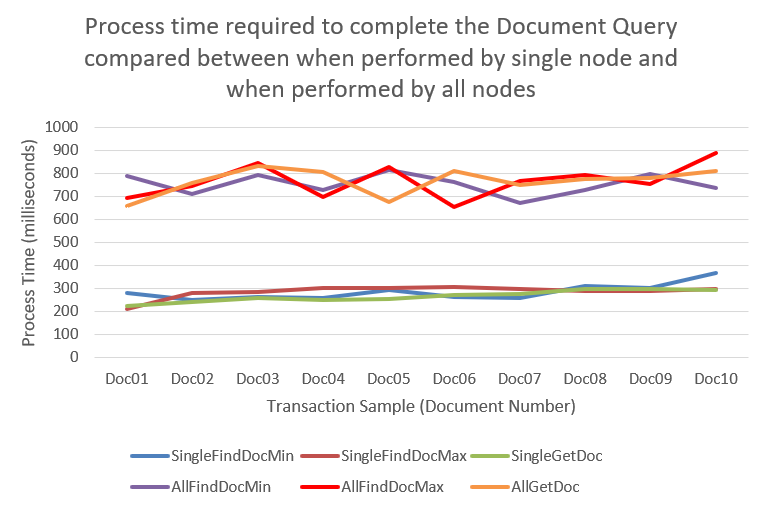


Figure 10 Processing time to complete Document Query compared between   
when performed by single node and when performed by all nodes

# Conclusion & Future Works

In this work, we achieve the system prototype for the XDS Blockchain which acts as the medium for health document sharing amongst the XDS Affinity Domain Network. The prototype was designed to be compatible with normal XDS Actors while also act as a medium for a common XDS network to interface with the IBFT Blockchain ledger. This enhances the IHE XDS.b Profile with the Blockchain characteristics while appreciating the network to further share their health document to further benefit from the network for both operational interoperability and cyber-security. However, due to the ever-changing nature of the software platform, further adoption of the implementation will need to be updated as the platform released newer version of the software to avoid version conflict of the source code.

In the implementation of the proposed concept, we excluded an XDS On-Demand Document Repository Actor and XDS Patient Identity Feed actor to reduce the complexity of the concept demonstration. For future work, those XDS Actors should also be implemented to the XDS Blockchain concept too. The XDS On-Demand Document Repository would enhance the benefit of the XDS Blockchain as it provides On-Demand health document type which gave flexibility and a wider range of usability of shared health documents to healthcare operation.

At the same time, The Patient Identity Feed Actor would aid the member of the XDS Affinity Domain Blockchain network by establishing the medium identifier for all members to seamlessly share their health documents. The Patient Identity Feed Actor may even further integrate into the SmartContract and eliminate the need for centralized identity feed in the network. Eliminate the cost which would be spent on maintaining the Patient Identity Feed Actor for the network.

Furthermore, the SmartContract also has the potential to become the exchange medium for ITI-43 transactions where the XDS Document Consumer negotiates with XDS Document Repository for retrieving actual health documents, allow health documents exchanging activities in the network to be recorded in the Blockchain ledger which could be further used in the incident investigation during the cyber-incident. These would maximize the potential of Blockchain technology implemented on the Cross-Enterprise Document Sharing Profile.

Other than the Cross-Enterprise Document Sharing Profile, the IHE IT Infrastructure is providing much more profiles and various tools for use in achieving healthcare interoperability. There remain a lot more possibilities of using the framework to maximize the potential of Blockchain technology and the future technology to come. As Blockchain technology still has a long way of development and research path to go through, the concept proposed in this work also could be further developed into a more advanced version for actual adoption in the future.

The source code of the project can be downloaded at URL.

# 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] 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).

[5] Paige Goodhew, “Why Healthcare Interoperability Matters | Redox.” https://www.redoxengine.com/blog/why-healthcare-interoperability-matters/ (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] HIMSS, “What is Interoperability?” https://www.himss.org/library/interoperability-standards/what-is-interoperability (accessed Apr. 27, 2019).

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

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

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

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

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

[15] “First known ransomware attack in 1989 also targeted healthcare.” https://www.beckershospitalreview.com/healthcare-information-technology/first-known-ransomware-attack-in-1989-also-targeted-healthcare.html (accessed Oct. 29, 2021).

[16] 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).

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

[19] “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).

[20] “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).

[21] “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).

[22] V. Puri, A. Kataria, and V. Sharma, “Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0,” *Trans. Emerg. Telecommun. Technol.*, p. e4245, 2021, doi: 10.1002/ETT.4245.

[23] 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).

[24] 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.

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

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

[27] 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.

[28] 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).

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

[30] 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.

[31] S. Tanwar, K. Parekh, and R. Evans, “Blockchain-based electronic healthcare record system for healthcare 4.0 applications,” *J. Inf. Secur. Appl.*, vol. 50, p. 102407, Feb. 2020, doi: 10.1016/j.jisa.2019.102407.

[32] A. Medical Association, “What is Information Blocking? Part 1.”

[33] 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.

[34] 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.

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

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

[37] 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.

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

[39] 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.

[40] “ethereum/go-ethereum: Official Go implementation of the Ethereum protocol.” https://github.com/ethereum/go-ethereum (accessed Jun. 05, 2021).

[41] “Installing Geth | Go Ethereum.” https://geth.ethereum.org/docs/install-and-build/installing-geth#install-on-ubuntu-via-ppas (accessed Jun. 10, 2021).

[42] “Command-line Options | Go Ethereum.” https://geth.ethereum.org/docs/interface/command-line-options (accessed Jun. 10, 2021).

[43] Quorum, “GoQuorum,” 2020. https://github.com/ConsenSys/quorum (accessed Jun. 03, 2021).

[44] “Install - GoQuorum.” https://docs.goquorum.consensys.net/en/stable/HowTo/GetStarted/Install/ (accessed Jun. 10, 2021).

[45] “Quorum 7-nodes Example.” https://github.com/ConsenSys/quorum-examples/tree/master/examples/7nodes (accessed Jun. 03, 2021).

[46] “ConsenSys/tessera: Tessera - Enterprise Implementation of Quorum’s transaction manager.” https://github.com/ConsenSys/tessera (accessed Jun. 05, 2021).

[47] “ConsenSys/constellation: Peer-to-peer encrypted message exchange.” https://github.com/ConsenSys/constellation (accessed Jun. 05, 2021).

[48] “quorum-examples/README.md at master · ConsenSys/quorum-examples.” https://github.com/ConsenSys/quorum-examples/blob/master/README.md (accessed Jun. 10, 2021).

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

[50] “Node.js.” https://nodejs.org/en/ (accessed Jun. 10, 2021).

[51] “npm.” https://www.npmjs.com/ (accessed Jun. 10, 2021).

[52] “web3 - npm.” https://www.npmjs.com/package/web3 (accessed Jun. 10, 2021).

[53] “xml2js - npm.” https://www.npmjs.com/package/xml2js (accessed Jun. 10, 2021).

[54] “fs - npm.” https://www.npmjs.com/package/fs (accessed Jun. 10, 2021).

[55] “net - npm.” https://www.npmjs.com/package/net (accessed Jun. 10, 2021).

[56] “util - npm.” https://www.npmjs.com/package/util (accessed Jun. 10, 2021).

[57] “moment - npm.” https://www.npmjs.com/package/moment (accessed Jun. 10, 2021).

[58] “cryptr - npm.” https://www.npmjs.com/package/cryptr (accessed Jun. 10, 2021).

[59] “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).