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

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

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

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

*Healthcare information sharing and interoperability between healthcare organizations are important factors to healthcare quality and safety since a patient may consult more than one specialist. Many challenges inhibit successful data sharing such as data integrity, security and privacy. Integrating Healthcare Enterprise (IHE) provides Cross-Enterprise Document Sharing (XDS.b) profile that allows the adopted organizations to share health documents between institutions. Security issues were not a focal point at the time of its inception. Healthcare domain has become a major target in emerging cyber-security threats. These threats increase difficulty to maintain secured health information sharing network. These cyberthreats can compromise integrity and availability of data and effect patient’s life. Blockchain technology can be used to solve health information sharing issues. A novel method using Blockchain technology to ensure health information integrity and availability is demonstrated, allowing health document sharing through decentralized network while addressing cyber-security issues through unique characteristics of Blockchain technology.*

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

# Introduction

(Shorten this paragraph, emphasize on the need of interoperability between healthcare organization)

On the increasing demand for better quality of healthcare services, operation efficiency pay important roles in patient services and economic outcomes. Healthcare information sharing and interoperability between healthcare organizations are one of major solutions to improve healthcare service quality. Patient’s health documents are scattered across different healthcare organizations, due to adoption of specialized healthcare informatics systems deployed by different organizations. Each healthcare organization has their own methods, processes, and workflow to handle healthcare information. This makes it hard for one health information system to interoperate with one another. Sharing health information with not fully trusted party exposing vulnerabilities to patients, business, and organization. The risk-reward ratio from sharing patients’ information with other may not be worthwhile if it were done improperly. . This create high friction for one organization to share their information with others. It even more difficult for individual patient to integrate and share their health information between different providers. It revealed that these interoperation problems cause huge decrease in efficiency on healthcare operation and result as lower quality of healthcare service [1] – [8]. This is why there are many initiatives that start to standardize healthcare information technology with the goal to allow healthcare organizations to be able to exchange patients’ information with each other. In this work we propose a solution that can solve data integrity and availabiltiyissues and reduce the friction of allowing health document sharing between different enterprises. By applying Blockchain technology on the Cross-Enterprise Document Sharing (XDS.b) Profile created by Integrating Healthcare Enterprise (IHE) initiative... (Existing solutions -> IHE XDS)

(Emphasize on scenario that will benefit from our work)

(Shorten this paragraph, emphasize on securing integrity of health information) (Lead to how our solutions can solve)

Sharing health information with not fully trusted party exposing vulnerabilities to business and organization. The risk that benefit the organization gain from sharing their patient information with other may not sustain the risk and cost they need to take. This create high friction for one organization to share their information with others.

Patients health and lives depend on their medical service provider. Failing to secure the service against cyber-attacks could cause great negative impact. Cyber-attacks that cause disruption of medical operation continuity like denial-of-service or ransomware, could result in the cost of patient’s life. At the same time, incident like data breached or information leakage could affect the reputation of the care provider if it disclosed to the public. It could further harm individual who is the information belonged to. It could even damage reputation and career of medical staff in the case of identity theft where identity of specific medical staff is used to perform the attack (such as credential theft, etc.). (End mentioning Blockchain)

(Introduction about existing technology addressing above issues then lead to remaining issues/problems/limits that still need further solution) (Mentioning Blockchain)

(Lead from those remaining issues to the need of our proposed solution which also emphasize on why we need Blockchain)  
 (Blockchain, its characteristics and impact) According to the document “Blockchain Technology Overview” which published by NIST, Blockchain can be informally define as a distributed digital ledger of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules. This give its characteristics to sustain threat against integrity and availability of information. At the sane time, with consensus as vital part of Blockchain, it allows members of Blockchain network to systematically “trusted” each other without the need of mutuality trust or physical agreement. Additionally, as distributed decentralized network, Blockchain require each member to passively share information with each other (One of famous Blockchain platform is Ethereum)

(There are existing works that try to combine Health Info. Exchange with Blockchain) -> MEDREC, Mayo  
However, there are some opening issues which we offer to solve. So, we propose (Our proposal, benefit, Why? How?) In this work we propose the solution that can solve interoperability issue and reduce the friction of allowing health document sharing between different enterprises altogether at once. By implementing Cross-Enterprise Document Sharing (XDS.b) Profile which published by Integrating Healthcare Enterprise (IHE) initiative, combined with benefit from Blockchain technology.

(Brief about other sections in this paper)

# RELATED WORK

## Health information sharing and Interoperability

(Explain more about the work, what they’ve done Why? How? Benefit)

Modern medical operation has large amount of healthcare information flow within the system. Throughout the ages, many medical provider services and organizations have deployed health information systems and databases to increase efficiency of operation in their medical services. As the time past, information of individual patients has scattered amongst different systems. This become new challenge for healthcare enterprise to further enhance their medical service efficiency by sharing health information with other healthcare providers. Many initiatives to standardize healthcare information sharing method have been published. (What idea of them that we adopt to our work How? Why?)

## Integrating the Healthcare Enterprise (IHE) and IHE Profiles

(Explain more about the work, what they’ve done Why? How? Benefit)

IHE is an initiative by healthcare professionals and industry to improve the way health information systems in healthcare share information. IHE promotes the coordinated use of established standards such as HL7 and DICOM to address specific clinical needs in support of optimal patient care. Systems developed in accordance with IHE communicate with one another better, are easier to implement, and enable care providers to use information more effectively. This helps enable seamless and secure access to health information that is usable whenever and wherever needed. An IHE profile provides use of existing standards, specifications, tools, and services for interoperability. IHE also engages clinicians, health authorities, industries, and users to develop, test, and implement standards-based solutions to vital health information needs. [19] IHE provides convenient and reliable way of specifying a level of compliance to standards enough to successfully reach efficient interoperability. (What idea of them that we adopt to our work How? Why?)

## Cross-Enterprise Document Sharing (XDS.b) Profile Implementation

The main goal of XDS.b profile is to allow enterprises that being a member of XDS Affinity Domain to discover shared health document stored in the system of other enterprise via 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. 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 consumers and users in the network to share health documents with each other efficiently.

## State of Cyber Security and Cyber Threats in Healthcare Domain

Patients’ health and lives depend on their medical service providers. Failing to secure the service against cyber-attacks could cause great negative impacts. Cyber-attacks that cause disruption of medical operation continuity like denial-of-service or ransomware, could result in the cost of patient’s life. At the same time, incident like data breached or information leakage could affect the reputation of the care providers if it disclosed to the public. It could further harm individual whose information belongs to. It could even damage reputation and career of medical staff in the case of identity theft where identity of specific medical staff is used to perform the attack (such as credential theft, etc.).

## Blockchain Technology

According to the document “Blockchain Technology Overview” which published by NIST, Blockchain can be informally defined as a distributed digital ledger of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules. This give its characteristics to sustain threat against integrity and availability of information. At the same time, with consensus as vital part of Blockchain, it allows members of Blockchain network to systematically “trusted” each other without the need of mutuality trust or physical agreement. Additionally, as distributed decentralized network, Blockchain require each member to passively share information with each other.

## Ethereum

Ethereum are one of well-known open source Blockchain platform. The platform initially invented by a developer named Vitalik Buterin and further develop by Ethereum community. Main approach of Ethereum Blockchain is about using Blockchain technology for applications other than cryptocurrency. The platform proposed concept about ‘smart contract’ which is equal to put computer program or algorithm into Blockchain ledger.

## Blockchain Related Work

There are many researches proposed about decentralizing healthcare information with Blockchain technology. The goal of decentralization and implementation of each work has variants. For example, the one that proposed by Mayo Clinic Institute is about using Blockchain network as central hub for health information exchange. They focus on using HL7 FHIR protocol to simplify information exchange method and use Blockchain as the middle for each member to communicate with each other. This allows auditability of health information exchanging and access trail. They also gave many suggestions about potential of using Blockchain to solve issue about interoperability. There is a work proposed by MIT named “MEDREC” which utilized Ethereum smartcontract to work as decentralized database for health information exchange. The work also proposed about utilizing data-anonymizing to allow the use of data shared within the Blockchain network in the field of data science which gave potential to enhance capabilities in medical research. However, due to the limit of the Blockchain itself, there still several issues and challenges to be addressed for Healthcare Information Blockchain to make it to reality.

# BACKGROUND KNOWLEDGE

# METHOD

This section describes a method of how the Blockchain was designed to operate under IHE XDS.b profile process flow. The first part introduces about architecture design and roughly defines how we integrate Blockchain components into IHE XDS.b profile process flow. The second part explains the first part further into the aspect of Blockchain components. This part focuses more on how we adopt and setup existing Blockchain platform to match our requirement for usage in our scenario. The last part further explains the first part in term of integrating IHE XDS.b profile with Blockchain. This part focuses on how we create and adapt each component in our work to meet the requirement specified by IHE XDS.b profile.

## Design Scenario (A Use Case?)

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

## Architecture Design

A requirement that needs to be setup to meet our scenario included type of Blockchain network, who is Blockchain participant node, and consensus which allow trustless publishing of block into the Blockchain ledger. In our scenario, we declare that participant node is machine hosted by members of XDS Affinity Domain which assume to be each hospital. Each Blockchain participant node will take the main role as XDS Document Registry actor which will maintain Blockchain ledger where document registry entry is kept. As the Blockchain allows only XDS Affinity Domain members to participate as node, this make the Blockchain type classified as permissioned chain. For consensus, it may need to be the consensus that can process large amount of Blockchain transaction at certain time due to continuous nature of medical operation. Smartcontract will be the main component that takes the role to keep all set of META-data attributes separated by each document, within Blockchain ledger. When Document Registry Searcher program was triggered by document user, the Searcher will perform iteration search on all META-data attributes set existing on the chain. All matched set will return to document user as list for the user to pick the one they needed. After the user picked the set they needed, user-side program will trigger smartcontract to return the whole set of META-data attributes of the selected set. Eventually, user-side program will use retrieved META-data attributes and repository URI to access actual document in its repository in hosting hospital.

# IMPLEMENTATION

This section will focus on technical explanation on concept implementation. The first part introduces about XDS Toolkit which is the source of XDS transaction sample for our implementation and act as validation tool to verify if our implementation complies to XDS.b profile. The second part will explain about technical setup of Blockchain platform for our implementation. The third part describes implementation of software that acts as component to integrate Blockchain to XDS.b process flow. This software behaves as the middle between function of XDS Document Registry actor and function as Ethereum Blockchain node. The last part will explain behavior of smart contract that we designed in technical aspect.

## XDS Toolkit

XDS Toolkit was provided by United States National Institute of Standards and Technology (NIST) [40]. The toolkit was developed to allow developers to test their software if it complies with IHE XDS.b profile and can communicate with other system. XDS Toolkit provide many tools that can send sample XDS transactions to specific location and wait for proper respond defined in XDS.b profile. These tools came in variant depend on what type of XDS actor that the testing software is.

## Blockchain Setup for Implementation

To directly command behavior of each Blockchain node, we require Geth client which allows user to issue command to the node like start-stop mining and start sync Blockchain data with other node. For programming smart contract, Ethereum providing IDE for Solidity language that can compile and deploy smart contract to local Ethereum node. To interface our program to Ethereum smart contract, we can use Ethereum API tools like Web3js [38] as a middle. Web3js allows smart contract control through Javascript language and transition variable from Javascript to Solidity. Then, Blockchain platform is ready for smart contract design and implementation of XDS.b profile.

## XDS Document Registry Actor

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

## Document Registry Smart Contract

Smartcontract was developed to store any kind of programming algorithm. So, we design smart contract which when executed, it will spawn smart contract that store given document META-data attributes value within number labeled smartcontract instances which encoded in Blockchain transaction. When these instances were called, it will return the stored metadata attributes value back. Allow the search program to identify the set. At the same time, this allow document registry to store within Ethereum Blockchain. These composed to function as Document Registry Smart Contract.

# discussion

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

[1] Carestream Health, “Interoperability : Connecting the Healthcare Enterprise to Deliver Responsive Patient Care,” pp. 1–9, 2015.

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

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

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

[5] Oracle, “Interoperability : A Key to Meaningful Use,” *Solutions*, no. November, 2010.

[6] HIMSS, “What is Interoperability?” [Online]. Available: https://www.himss.org/library/interoperability-standards/what-is-interoperability. [Accessed: 27-Apr-2019].

[7] Paige Goodhew, “Why Healthcare Interoperability Matters | Redox.” [Online]. Available: https://www.redoxengine.com/blog/why-healthcare-interoperability-matters/. [Accessed: 27-Apr-2019].

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

[9] A. Le Bris and W. El Asri, “STATE OF CYBERSECURITY &amp; CYBER THREATS IN HEALTHCARE ORGANIZATIONS Applied Cybersecurity Strategy for Managers,” *ESSEC Bus. Sch.*, p. 13, 2017.

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

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

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

[13] B. Weinelt, “Digital Transformation of Industries. Logistics Industry,” no. January, 2016.

[14] A. Marcelo, D. Medeiros, K. Ramesh, S. Roth, and P. Wyatt, “Transforming Health Systems Through Good Digital Health Governance,” *adb Sustain. Dev. Work. Pap. Ser.*, no. 51, pp. 1–15, 2018.

[15] T. Shaw, M. Hines, and C. Kielly, *Impact of Digital Health on the Safety and Quality of Health Care*, vol. 5, no. January. 2000.

[16] Cisco, “The Digitization of the Healthcare Industry: Using Technology to Transform Care,” *Cisco*, vol. 1, p. 12, 2017.

[17] G. Bullhound, *Digital healthcare*, no. November. 2015.

[18] B. Meskó, Z. Drobni, É. Bényei, B. Gergely, and Z. Győrffy, “Digital health is a cultural transformation of traditional healthcare,” *mHealth*, vol. 3, pp. 38–38, 2017.

[19] IHE International Inc, “About IHE.” [Online]. Available: https://www.ihe.net/about\_ihe/. [Accessed: 11-Sep-2018].

[20] IHE International Inc, “IHE Process.” [Online]. Available: https://www.ihe.net/about\_ihe/ihe\_process/. [Accessed: 11-Sep-2018].

[21] IHE International Inc, “Profiles.” [Online]. Available: https://www.ihe.net/resources/profiles/. [Accessed: 17-Sep-2018].

[22] 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.

[23] dkorolyk, “What Is The Difference Between XDS,XDS.a,XDS.b and XDS-I?,” 2012. [Online]. Available: http://healthcareitsystems.com/2012/05/22/what-is-the-difference-between-xds-xds-a-xds-b-and-xds-i/. [Accessed: 17-Feb-2019].

[24] M. N. Luke, S. J. Lee, Z. Pekarek, and A. Dimitrova, “Blockchain in Electricity: a Critical Review of Progress to Date,” pp. 1–36, 2018.

[25] PwC, “a Catalyst for New Approaches in Insurance.”

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

[27] D. Yaga, P. Mell, N. Roby, and K. Scarfone, “Blockchain Technology Overview (NISTIR-8202),” *Draft NISTIR*, p. 59, 2018.

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

[29] A. Ekblaw, A. Azaria, J. D. Halamka, A. Lippman, I. Original, and T. Vieira, “A Case Study for Blockchain in Healthcare: " MedRec " prototype for electronic health records and medical research data,” *IEEE Technol. Soc. Mag.*, pp. 1–13, 2016.

[30] 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.

[31] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, “Blockchain-Based Data Preservation System for Medical Data,” *J. Med. Syst.*, vol. 42, no. 8, pp. 1–13, 2018.

[32] “ÐΞVp2p Wire Protocol.” [Online]. Available: https://github.com/ethereum/wiki/wiki/ÐΞVp2p-Wire-Protocol. [Accessed: 26-Apr-2019].

[33] 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.

[34] 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.

[35] yutelin, “Istanbul Byzantine Fault Tolerance.” [Online]. Available: https://github.com/ethereum/EIPs/issues/650. [Accessed: 09-Apr-2019].

[36] Jim Zhang, “Consensus Algorithms: PoA, IBFT or Raft? - Kaleido - Kaleido,” 2018. [Online]. Available: https://kaleido.io/consensus-algorithms-poa-ibft-or-raft/. [Accessed: 09-Apr-2019].

[37] “Quorum | J.P. Morgan.” [Online]. Available: https://www.jpmorgan.com/global/Quorum. [Accessed: 26-Apr-2019].

[38] nivida, “Web3js Ethereum javascript API.” [Online]. Available: https://github.com/ethereum/web3.js/. [Accessed: 26-Apr-2019].

[39] S. Bragagnolo, H. Rocha, M. Denker, and S. Ducasse, “Ethereum query language,” *2018 IEEE/ACM 1st Int. Work. Emerg. Trends Softw. Eng. Blockchain*, pp. 1–8, 2018.

[40] United States National Institute of Standards and Technology, “NIST Document Sharing Test Facility.” [Online]. Available: http://ihexds.nist.gov/. [Accessed: 27-Apr-2019].

*On the increasing demand for better quality of healthcare service, there is the topic that involve healthcare information technology in term of operation efficiency.*

*There found initiatives to standardize healthcare information sharing method. To address issue about health document sharing between different enterprises, Integrating Healthcare Enterprise (IHE) initiative have proposed Cross-Enterprise Document Sharing (XDS.b) Profile. The profile allows the adopted organizations to share health document between each other simultaneously. At the same time, as well as other industry, there also emerging cyber-security threats threatening healthcare information domain. These threats increase difficulty to development of health information sharing network and causing damage to healthcare enterprises. These cyberthreats can cause damage to the industry in many aspects, especially those cyber-attack that targeting integrity and availability of data. These kinds of cyber-attack can severe the continuity of medical operation which could result as the cost of patient’s life. There are many solutions technology proposed to deal with these kinds of cyber-attacks. One of the technologies that on the trend to deal with cyber-threats threatening integrity and availability of data is Blockchain technology. There are several research and concepts that proposed about using Blockchain technology to solve health information sharing issue. But there still many limits prevent Blockchain technology to effectively integrated with data like health information. In this work, we propose another approach for integrate Blockchain technology with health information. We see that standard like IHE XDS.b profile could be use with Blockchain technology to allow health document sharing through decentralized network while address cyber-security issue through unique characteristics of Blockchain technology.*