Framework for Data Management in Public Service Delivery Applications in Sri Lanka Using Blockchain Technology

By

G.W.N.T. Deshapriya 2013 IS 010
G.H.G.M. Dharanidu 2013 IS 011
J.A.R.T. Jayakody 2013 IS 023

This dissertation is submitted to the University of Colombo
School of Computing
In partial fulfillment of the requirements for the
Degree of Bachelor of Science Honours in Information Systems

University of Colombo School of Computing
35, Reid Avenue, Colombo 07,
Sri Lanka

January 2018

Declaration

We certify that this dissertation titled “Framework For Data Management In Public Service Delivery Applications In Sri Lanka Using Blockchain Technology” is entirely our own work and it does not incorporate, without acknowledgement, any material previously submitted for a degree or diploma in any university and to the best of our knowledge and belief, it does not contain any material previously published or written by another person or our self except where due reference is made in the text. We also hereby give consent for our dissertation, if accepted, be made available for photocopying and for interlibrary loans, and for the title and abstract to be made available to outside organizations.

Candidate Name: G.W.N.T. Deshapriya Registration No: 2013 IS 010

……
Signature of Candidate Date: 25.05.2018

Candidate Name: G.H.G.M. Dharanidu Registration No: 2013 IS 011

……..
Signature of Candidate Date: 25.05.2018

Candidate Name: J.A.R.T. Jayakody Registration No: 2013 IS 023

……
Signature of Candidate Date: 25.05.2018

I, Dr. M.D.J.S. Goonethillake, certify that I supervised this dissertation entitled “Framework for Data Management in Public Service Delivery Applications in Sri Lanka Using Blockchain Technology” conducted by

Ms. G.W.N.T. Deshapriya,

Mr. G.H.G.M. Dharanidu and

Ms. J.A.R.T. Jayakody

in partial fulfillment of the requirements for the degree of Bachelor of Science Honours in Information Systems.

……

Signature of Supervisor Date: 25.05.2018

Abstract

This Dissertation will comprise details of the research “Framework for Data Management in Public service delivery applications in Sri Lanka using Blockchain technology”. Blockchain technology is an emerging technological concept which shows the capability of addressing many problems in many different domains, including the public-sector domain which is considered for this research. How four prominent data management issues namely data accessibility difficulty, data manipulation possibility, data loss and privacy preservation of data is mitigated through the applicability of blockchain technology are the research questions that are answered in the research. In order to derive a common framework, three distinct data management processes were used namely Birth Marriage and Death certificate management system, Land title management system and eHealth records management system. Systems were redesigned using blockchain technology and prototypes developed using two different existing platforms and qualitatively evaluated for the four criteria of research questions. Based on the characteristics extracted from the selected systems, a Generic Guideline was designed comprising the six areas that need to be considered when adopting a blockchain for Data Management in a Public Service Delivery application and five steps that should be followed in adopting a blockchain for the specific needs of the government institution.

Preface

In this dissertation, the Chapter 3 designs are based on the information gathered from Land Registrar's Department, District Secretariat Offices and Information and Communication Technology Agency, Sri Lanka. The Generic Guideline is the contribution of this research based on the developed designs and existing literature. All 3 redesigned systems are created by the effort of three members of research and our supervisor. For the development of prototypes in Chapter 4, components from two existing blockchain platforms were taken namely, Multichain and Hyperledger Composer.

Acknowledgement

Firstly, we would like to express our sincere gratitude our supervisor Dr. M.D.J.S. Goonethillake, Senior Lecturer at University of Colombo School of computing for her valuable support and contribution in our research and the dedicated guidance provided to us throughout the research in terms of motivation, and immense knowledge.

Our sincere thanks go for the resource personnel of Information and Communication Technology Agency Sri Lanka (ICTA) for their dedication in information on e-government initiatives that laid basement for our research. And specially Mr. K.Wickramasuriya, project officer at Information and Communication Technology Agency Sri Lanka (ICTA) for his valuable support in assisting us to organize informative sessions to gather valuable insight on the existing e-government initiatives and projects.

We would like to thank the representatives from the Land Registrar's Department Colombo, Divisional Secretariat Office Timbirigasyaya and Divisional Secretariat Office Kesbewa, for sparing their valuable time and providing us the information about the current status of data management in the respective local government bodies. And specially Mrs. M.Wanigasekara, Assistant Divisional Secretary, Thimbirigasyaya Divisional Secretariat and Mrs. P. Dissanayake from Kesbawa Divisional Secretariat for their valuable time and effort to guide us through the internal processes of those respective government organizations.

Last but not the least, we thank our families and fellow colleagues for their precious support given to us throughout this period to help us successfully complete the research work.

Table of Contents

List of Figures

List of Acronyms

ACL - Access Control List

ATM - Automatic Teller Machine

BEV - Blockchain enabled e-voting

BMD Project - Birth Marriage Death Certificate Management System

CLI - Command Line Interface

DAO - Decentralized Autonomous Organization

DS Office - Divisional Secretariat Office

eHealth - Electronic Health

eVote - electronic Vote

eLand Registry System - Current Land Title Management System

HHIMS- Hospital Health Information Management System

ICTA- Information and Communication Technology Agency

ICT4D - Information & Communication Technology for development

IoT - Internet of Things

IP - Internet Protocol

KB - Kilo Bytes

MB- Mega Bytes

PID - Unique key for a patient in the HHIMS System

PoW - Proof of Work

PoET - Proof of Elapsed Time

RRRN No- System name for Daybook No.

SPOF- Single Point of Failure

SQL- Structured Query Language

RDBMS- Relational Database Management System

Chapter 1 - Introduction

1.1 Background to the Research

In Sri Lankan government institutions, public data is stored and managed on behalf of public. Certificate issuing agencies such as Land registry department, District Secretariat, Department of registration of persons store critical public data which are used in verification purposes. So the integrity of the data in such certificates is crucial. When requesting a copy of Birth certificate, marriage certificate or a death certificate any citizen should go to the district where the incident registered to obtain the copy [1]. Though Lifetime Internal Migration between districts happens in a higher rate and every citizen should visit the original District Secretariat to get service done [2]. Copies of Land title registration certificates are also issued in the same district where the property is located. Since there is a central authority to be trusted, forging is considered to be possible. When cross checking the validity of these certificates always there is a concern about the originality of the documents making the process much difficult and complex. Incidents of producing illegal certificates including false birth, marriage, death, real estate ownership certificates is commonly reported in Sri Lanka [3] due the absence of a real time tracking of the modification of data. Due to the data management practices followed in the government organizations the vulnerability for frauds and theft is inevitable arising the need to adopt a much secure mechanism especially in areas like proof of ownership of land registries, property titles, or any type of real estate ownership where keeping the chain of custody for physical asset is important. Stored data has a threat to be lost due to natural disasters and physical damages to properties. Because of natural disasters such as Floods, Landslides and Tsunami documents get destroyed. Many similar incidents occurred in Sri Lanka recently. There are some specific data which needs specific privacy concern regardless of being public data. Hospital and patient data are an example of such data. Unauthorized exposure should be blocked for such data.

For the data management in public entities, computerization of records is initialized under e-government transformation. Computerization of Birth, Marriage and Death certificates are done under the BMD project. Computerization of land title information is done under eLand registry project. Health data of government hospitals is computerized under eHR project [4].

For storage and data management, database options as Centralized databases and Distributed databases are used.

Public data management has prominent problems such as accessibility difficulties when receiving service, possibility for fraud and error and data loss possibility. However through any of those database solutions cannot provide a single option to address all problems at once. A centralized database may accomplish the challenge of geographical difficulty, but since there is a data loss possibility unless a backup is kept. Since a central authority is there, a malicious Database Admin could alter data in the source. A decentralized database may promise the geographical independence, however if a node is down with failure data in that node will be unavailable unless replication is done. If full replication is done, data availability can be promised, but maintenance is costly. For all of the mentioned database solutions security should be implemented as a separated layer as it is not available as an inbuilt feature. Therefore expert ideas needed and it costs an extra effort. When designing a DBMS threat is not modelled. Audit trails are needed to monitor user actions. However audit trails are not inbuilt, extra effort is needed for implement and audit trail is not a precaution mechanism [5].

Among potential solutions, Blockchain [6] is a trending concept that shows its capability to cater for a better storage medium, a distributed ledger. Therefore the applicability of Blockchain technology to serve public data management in Sri Lanka is worth to be explored.

1.2 Research Problem and Research Questions

The main objective of the research is to design a framework for public data management using Blockchain technology. It is based on the main research problem of "How to use Blockchain Technology to mitigate data management issues in public data management in Sri Lanka". The research problem is further segregated into 4 research questions as,

Q1: How to reduce the data accessibility difficulties in public data management systems using blockchain technology?

Due to geographical and technical barriers the accessibility to public data has become a greater concern. Even with the use of computerized records of the data, current procedure in

Sri Lanka need the requester to be present in the specified government agency. Since the data accessibility is a major concern for public delivery systems, the prototype block solution will be designed in a way that it could reduce the accessibility and availability issues of the existing solutions. In this research a framework is to be designed to overcome this problem by taking into account the decentralized nature of Blockchains.

Q2: How to reduce the possibilities of data management frauds and errors using blockchain technology?

Data manipulation frauds are one of the most critical problems that is faced by modern data management systems. As it is described earlier most of those public systems handles critical data so that the security levels should be very high. Most of the existing data management solutions are focused on detection of those fraudulent activities rather than preventing those activities. We will be focusing on how Blockchains can be used in such systems to prevent data misuse rather than detecting fraudulent activities.

Q3: How to reduce the data loss possibilities using blockchain technology?

With respect to this issue, our main focus will be on identifying the capabilities of Blockchains that could be used in an event of system failure. Even though several data recovery techniques are available still Sri Lankan public service delivery systems have great concerns about data recoverability. Most of those government organizations handle critical public data; so the data recoverability options should be very effective in an event of a failure or a disaster. We will be focusing on how Blockchains can be used in such systems to recover the lost data effectively.

Q4: How to cater Privacy Preservation using blockchain technology?

There are public data which needs specific privacy measures regardless of being public data. Patient data under hospital data will need more privacy than a verification document data. For that, the capability of blockchain to act as a mediator to limit access to sensitive public data is to be utilized. To address the privacy issues of data, controlling access to data using properties of blockchain is considered here.

1.3 Justification for the research

Even Though computerization of public data is done under e-government initiatives [4], there are data management issues that cannot be fully addressed through a typical database solution. Accessibility concerns, data manipulation possibility, data loss and privacy preservation of data are prominent concerns for the public data management. Security should be implemented by incurring an additional effort, if a typical database solution is used. Blockchain is a novel concept which was initially used as the underlying technology of Bitcoin cryptocurrency [7]. Its potential ability of data storage is a trending research topic. Security is not needed to be implemented separately because it comes as an inbuilt feature in Blockchain. In Sri Lankan context, no researches have been conducted to find the ability of a blockchain to cater data management. Therefore, there is a research opportunity. So in the research, the exploration was done on the applicability of Blockchain technology to public data management and the possible methods of incorporating it to mitigate data management issues.

1.4 Methodology

The research is a Qualitative research which followed in the following approach

1. Studying current Public Data Management Systems and identifying the existing challenges in delivering value to general public
2. Investigation of the features of blockchain technology to address challenges in public data management systems, which cannot be addressed through current database solutions
3. Identifying three public data management systems which would utilize the properties of blockchain technology to create value by resolving issues in their current systems
4. Designing of three selected data management systems using blockchain technology
5. Designing an abstract guideline/framework by selecting properties from the selected data management systems
6. Evaluating the Abstract Design for the identified challenges of Data Accessibility, Data Availability, Possibility of fraud and error and Privacy Preservation.

1.5 Outline of the Dissertation

The dissertation will be comprised of six chapters. First chapter will cover the introduction to research, the research problem, scope and a brief explanation of research approach. Second chapter will be comprised of the detailed literature review conducted for the research. The third chapter will explain the research design and the drafted designs for the data management systems after incorporating Blockchain technology. Fourth chapter will include the implementation details of prototypes for the research. Fifth chapter covers the research findings and evaluation while sixth chapter will be the conclusion of research.

1.6 Research Scope

The research considers the data management of public service applications in Sri Lankan government. To design the processes to express how to create the framework to address the challenges in public data management, 3 distinct public data management systems are considered namely, the Birth Marriage and Death Certificates Management in District Secretariat offices, the Land Title Management System in Land Registry Departments and the Hospital Data Management System in Government Hospitals [4]. The 3 systems are selected to elaborate the possible value addition to public data management through the properties of Blockchain Technology. Through the design of 3 systems with blockchain, suitable abstract design is to be extracted from the properties identified. The abstract Design is to be evaluated for the fulfillment of challenges of public service delivery, data management systems. The criteria for the evaluation will be the Data Accessibility, Data Availability, Possibility of fraud and error and the privacy preservation.

1.7 Conclusion

This chapter laid the foundation to the dissertation through explaining the research problem that is tried to addressed, the scope and the research approach. The research approach will be more descriptively explained in future chapters.

Chapter 2 - Literature Review

Governments store and issue public data at the request of the general public such as Birth, Marriage, Death certificates, Land entitlement certificates, Vehicle registration information, Revenue license information and National Identity cards etc. Due to the usage of such information for verification purposes accuracy, availability and efficient delivery of these data is required and important. Under e-government initiatives, many countries have started computerization of these data with usage of many database solutions such as centralized databases, distributed databases, Virtual Private databases and Cloud database solutions. This computerization has reduced the possible malpractices in the paper based storage to some extent. However, the tampering of data and forging is still possible even with these database solutions. Along with the development of technology, data management solutions have emerged with the capability of providing more secure and credible interactions with new innovations of technology.

Blockchain technology was introduced as the underlying technological infrastructure which enabled the functions of the digital currency, Bitcoin [7]. Blockchain technology was first used to store financial transactions, but later it was identified as a technology that could be used to store anything of value in the shared ledger. Blockchain is a decentralized, peer to peer network of nodes. In Blockchain the data is attached to a chain in a chronological way based on the hash value which is embedded in the header of the block. So changing data of a block should have followed with a proof of work of all the previous blocks. And in a Blockchain the longest chain is accepted to be the genuine chain. These properties of Blockchain make it tamper-proof and data loss resistant. It ensures the credibility of data stored in it [8]. Since the integrity and availability of public data is crucial, a Blockchain has the potential to be a better storage mechanism for such data.

2.1 e-government and data management

Data management of public data such as Birth, Marriage, Death certificates, Land entitlement certificates, Vehicle registration information, Revenue license information and National Identity cards is considered important for any country. These data are stored in government institutions and issued at request of general public. These documents cater verification purposes in many instances. Other than the verification documents, governments

store data like health data in government hospitals for management purposes. In government reform through e-government, many countries have initialized computerization of paper based public data sources to ensure better management.

The recent case study which was published in 2017 “One-Stop-Shop Public Service Delivery Model: The Case of Georgia” [9] mentions that The Ministry of Justice of Georgia identified the development of an effective civil registration system is a crucial requirement in reform of country. Identification documents digitization researches and projects were carried out in many counties. Asian Development Bank’s working paper “Public Service Delivery: Role of Information and Communication Technology in Improving Governance and Development Impact” [10] mention about the “Aadhaar” certificate computerization program which stores Biometric information of “Aadhaar” holders in a central database, carried out in India. The unique identity number of “Aadhaar” is the verification to get access for entitlements to the poor for subsidized food, fertilizer, and health services which makes the management of data critical. Article “One-Stop-Shop Public Service Delivery Model: The Case of Georgia” [9] mention how The Civil Register Agency in Georgia digitized birth and death civil act certificates from its archives and simplified passport and ID issuance services. Integration of citizens’ database to various public and private entities enhanced information sharing and security establishment. As security measures biometric parameters was added to minimize the potential to forge personal ID documents, database monitoring system and database protection system implemented to secure data from unauthorized access and track database in order to minimize untargeted use of identification data and to avoid data damage. In Sri Lanka, ICTA has an ongoing project named BMD [4] which the digitalization of Birth Marriage and Death certificates is done. In BMD project, the paper based Birth, Marriage and Death certificates stored in all Divisional Secretariat offices are scanned and stored in a centralized database. In the BMD project, the databases and software to query the database to find the certificate is introduced. The developed application facilitates the search for a certificate by its reference no, birthplace or a specific field like mother’s name.

Land entitlement documents digitization projects and researches done under e-government initiatives to keep solid understanding of chain of custody and the properties of real estate. The article “Importance of development context in ICT4D projects: A study of computerization of land records in India” [11] discuss about the computerization of land records project “Bhoomi” which was conducted in Karnataka of India in 2001. The Record of

Rights, Tenancy and Crops (RTC) certificate verifies the ownership of land, location of it, unique identity number of land, crops cultivated on the particular land, identity of the tiller and loans taken for the land. “Bhoomi” centralized database was created to cater the storage purpose. The case study “Electronic Integration of BHOOMI with Stakeholders, Karnataka” [12] is an extension of previous “BHOOMI” land records computerization program. It explains the integration done to enable data sharing among different stakeholders in real estate management domain. Under the e-governance program BHOOMI database was integrated with the registration software, “KAVERI”, “BHOO SWADEENA” Land acquisition processing software and Banks. The World Bank Conference report “Innovations in Land Information Recording, Management and Utilization in Sri Lanka” [13] presents the land deeds computerization system “Bim saviya” which is implementing in Sri Lanka. In project, a Land Information Database with a digital Land Information System will be the base for efficient and scientific Land Management where the digitized system facilitates searching for a land by name, owner’s name and other critical parameters. The land Information Database will be integrated for data sharing with Banks, Financial institutions, lawyers, notaries, utility companies and many other administrative, service oriented and commercial bodies in order to reduce fraudulent practices.

Though computerization of records is done under e-government reforms, all database solutions need to implement security as a separate layer. According to recommendations “Report of Committee on Computerization of Land Records” [14] of Department of India, “Bhoomi” project needs to implement security measures to be reliable. Provisioning backup for SQL database, backup storage managing under an official, implementing both physical and cyber security, implementing policy for confidentiality, accountability, access control and data access over network, and scheduling security audits should be carried out. Database solutions also subject to data loss vulnerability and data manipulation if not well maintained. In 2016 there were 269 data breaches occurred in government institutions and from all data breaches occurred from 2013 11.46% were directed to government institutions [15]. If a centralized database is used, there is a centralized authority who is in charge of the database who possess power to manipulate database and forge records or delete records. In a government organization people with power could misuse this property which makes the solution non reliable. If a distributed database is used, when one node is down, data stored there would be in lost unless a replication exists. If a cloud database is chosen, there is also a third party to be trusted for the integrity of data and unauthorized data modification is possible via a cyber-attack. Therefore,

every database solution possesses a significant vulnerability in the management of public data. No single solution will possess power to provide distributed access, data availability and data integrity.

Apart from data security, in the areas such as public health record management preserving privacy has become the main issue. Along with the e-government program ICTA has initiated an e- health program to computerize the public health records as well. Currently ICTA has implemented an open-source medical records handling system. The system is designed to replace paper records while covering all the clinical related areas such as lab tests, drug issuance processes and report generations. At present the system is implemented across nineteen clinics with standalone databases. In the international context several researches have been done in order to address the privacy concerns in large scale health related data management systems. In the research conducted by B. Sangeetha et al. [16], they have explored the capabilities of protecting privacy in a cloud based environment. In the process they have developed a novel framework where the patients can encrypt their medical data when uploading to the cloud. Ability of using multi key approach in the cloud based environment is also examined by Poonam Patel, Amar Buchade [17]. This research also highlights that existing techniques are not capable of providing complete privacy. A similar privacy protection approach using symmetric ciphers and asymmetric ciphers has been implemented by Kong G and Siao Z [18]. They have directly addressed the scalability concerns while addressing the privacy issue with a composite privacy protection approach.

2.2 Blockchain

2.2.1 Bitcoin

The Blockchain concept established with the arrival of cryptocurrency, Bitcoin. There is no central authority to govern the bitcoin network. Satoshi Nakamoto presented the initial idea of Bitcoin in his paper “Bitcoin: A Peer-to-Peer Electronic Cash System” which was published in 2008 [7]. According to the paper, bitcoin is a purely peer-to-peer version of electronic cash that would allow online payments to be sent directly from one member to another without the mediation of a financial institution like a bank. In bitcoin, an electronic coin represented as a chain of digital signatures. Each owner transfers the coin to the receiver by digitally signing a hash of the previous transaction and the public key of the next receiver

and adding these to the end of the coin. Double-spending of bitcoins in a user wallet is blocked with the use of a peer-to-peer network. The special nodes of the network which called as ‘miners’ validate the transactions and ensure the credibility through a proof of work called as ‘mining’. Network timestamps transactions and arrange them in a chronological order by hashing them into a chain structure. Forming a record of transaction is impossible without redoing the proof-of-work making the security aspect become stronger. Changing content of a transaction is create a block of data and it should have the hash value of the previous block of data to be accepted by the chain. Genuine transactions are verified in that way. The longest chain of data blocks is considered as the correct chain and all the nodes automatically downloaded it when they join the network. Unless 51% of the nodes are belonged to one party, tampering and attacking data is impossible [19]. The network requires minimal structure where messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone. The underlying technology which provides operation of the bitcoin is the blockchain [6].

2.2.2 Blockchain Concept

A blockchain can be simply defined as a distributed ledger where all the transactions or digital events that have been executed and shared among participants through a peer-to-peer network. Applicability of this technology has expanded across a vast range of application areas such as documents, contracts, properties and assets. With the exponential breed of this technology the researchers have sub categorized those possible application areas into three parts mainly. Blockchain 1.0 is referred to electronic currency or fund transfers where Blockchain 2.0 is referred to various types of contracts. And the researchers have introduced Blockchain 3.0 as the applications which are used beyond currency such as government, health, science related applications [20]. Blockchain utilizes a cryptographic code without the interactions of the human which will guarantee the security aspect of the information against the risk of fraud and alterations. Hence this technology reflects exceptional benefits in terms of automation, auditability, transparency, security and cost effectiveness.

2.2.2.1 Blockchain Technology

The blockchain can be defined as an application layer that will act as a tier enabling the existing stack of Internet protocols to run on it and allow more complicated financial contracts or other types of transactions. Any user who is willing to join an existing Blockchain will have to install a blockchain application in their own servers or computers. Since blockchain is a distributed database every single user will have of their own complete copy of the database. The integrity and the chronological order of the blockchain are enforced with cryptography. Anyone can request that any transaction or a record to be added to the blockchain, but transactions are only accepted and added to the blockchain only if more than 50% of users of the network agree on that it is a valid transaction [20]. This agreement is based on a checking, which is done reliably by each and every user, creating a very fast and secure ledger system that is remarkably tamper-proof. So there are no central authorities existing within a blockchain. Each and every verified transaction in a blockchain should be bundled with other recent transactions and embedded in a 'block'. Then this newly created block will be added to the longest existing chain within the network.

The process of adding a new block to the existing blockchain will be called as "mining." Any user within a blockchain network can become a miner. But due to the high levels of resource requirements the number of miners within a network remains low. Usually the miners engage in a process of solving a complex mathematical problem and the first miner who is capable of identifying the solution for the problem will be rewarded according to the predefined methods. There are various means to pay incentives to the miners as well. Usually in Blockchains the miners will be rewarded with a predefined number of blocks for a single block and will be paid some transaction fee as well. Thus the Blockchain constantly grows as miners add new blocks to the chain to record the most recent transactions. The blocks are added to the blockchain in a linear, chronological order and transmitted all over the nodes of the network. Once the data is entered into the blockchain, those data cannot be altered or deleted in the original place. That is because of the "append only" feature in Blockchains. Modified data will be added to a separate block in the chain. So the auditability of the valid transactions are ensured automatically.

2.2.2.2 Block in blockchain

Block is the basic organization unit of data in the blockchain. The very first block in the blockchain is called as the Genesis Block [21] and it is always hard coded to establish the chain. A block consists two parts namely, block header and body. Block header contains the hash value of previous block, block size, a random Nonce value, Block height which defines no of precedent blocks, hash of Merkle root, timestamp of creation time of block and number of transactions included in the block. The body contain non empty transactions or records. Blocks are linked by the hash values of previous block. If the hashes are not matching, the blockchain breaks from that point and it is used to identify non genuine transactions. [22]

2.2.2.3 Merkel Tree in blockchain

Merkel root is the component that vouch for the integrity of individual records or transactions included in the block. The transactions are first individually hashed. Then they are combined and hashed in a tree like order. The top level is named as the Merkel root which is created using the systematic hashing combination of all transactions [23].

Illustration of Merkle Tree

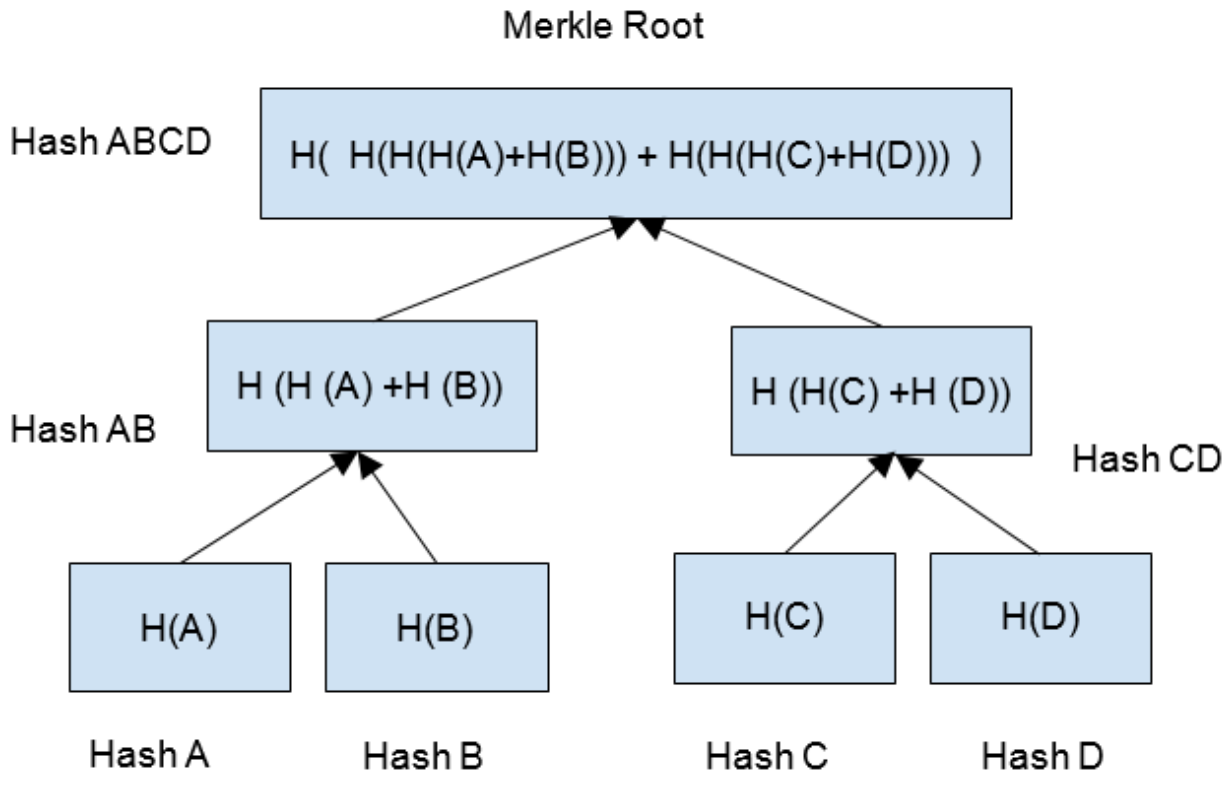


Figure 1- Illustration of Merkle Tree

2.2.2.4 Mining & Consensus

In distributed ledgers the protocol that is being used to create the consensus among the participants which determine how the transactions will be accepted to the ledger is one of the basic component. Consensus can be defined as the process that build the agreement between the participants who are included in the network. Different algorithms have been introduced by considering the variety of requirements arise due to the concerns on the performance, scalability, threat factor and the failure model [24].

When considering these algorithms in order to achieve the consensus with arbitrary faults generally, a voting process is carried out between a set of known participants. Currently there are several existing approaches which can be identified, to determine the group consensus. In the blockchain protocol, a form of consensus call the Nakamoto consensus [7] is achieved with the help of a set of participants known as "miners" who are distributed across the network. These miners are responsible for the collection and the validation of the cryptographically signed transactions from the other nodes in the network and generating the blockchain. Since the blockchain network is decentralized, the participants are connected peer-to-peer with the possibility of generating simultaneous blocks that will create a risk of breaking the single chain structure concept of Blockchain. It's being resolved by yet another mechanism which decide on what branch to select based on a concept called "longest chain". But in case of an attack, the attackers will be able to generate blocks to be attached into the blockchain before any other legitimate miner, thereby forcing the acceptance of the faulty branch. But it's being addressed by including a proof that will show the other participants in the network that the creator of the particular block has performed some approved amount of work on the block. This value is known as the Proof of Work (PoW) which will be included in every valid block for verification and validation process.

Normally proof-of-work is been implemented in the form of cryptographic puzzles. For example, in the Bitcoin cryptocurrency a miner in the network must change a variable value called "nonce" value included in each block until the cryptographic hash value of the block is smaller than the predetermined threshold value of the blockchain network. This involve testing the nonce values by brute force until the miner get a cryptographic hash value less than predetermined threshold due to the properties of the hash value. The miner who finds the Nonce

value at the earliest will broadcast the specific block to the rest of the nodes in the network who will thereby accept the block and add it to their own copy of the blockchain.

This effort that needs to be incur on a particular block will make the block itself a "proof-of-work" which contain a nonce value which represent a correct solution to a crypto puzzle. In practical situations various hash functions are being used to cater for different difficulty levels required by various systems that will stress the amount of load in the processors and the memory of the computing devices that will be used for mining purposes. The difficulty can be set according to the required expected rate of block generation by the miners with the use of a particular deterministic algorithm.

Many cryptocurrencies that uses blockchain technology adopted using the Proof of Work (PoW) mechanism which actually act as a robust solution to select the consensus leaders as well as to deploy the reward distribution include in the blockchain based cryptocurrencies like Bitcoin. When considering a system implemented using Proof-of-work, miners in that particular blockchain network can only lead in the consensus rounds with proportion to the amount of computational resources they possess. Even Though this provide the solution for the any problem that might occur due to the gaining of majority power within the network and manipulating the data that is being entered into to the Blockchain it raise other concerns with relevant to the huge monetary and environmental costs [25].

Proof of Elapsed Time (PoET) can also be stated as a Nakamoto-style consensus algorithm that is being designed to be a production-grade protocol capable of supporting large network populations. For achieving the distributed consensus, according to the literature there need to be several characteristics embedded in such type of consensus algorithms. It should be capable of distributing the election across the network irrespective of the possible amount of population or the participants in the network which reflect the fairness in the process. And also the value that is being generated by the control over the process should be proportionate for the investment and the cost associated with it. And the other nodes should be able to do the verification without much effort in a simple manner and also in less time to confirm whether the election was legitimate.

When considering the PoET algorithm it is designed in a way that it will achieve the above mentioned critical characteristics using the new secure CPU instructions which are

becoming widely available in the recent consumer and enterprise processors. PoET works in a way where every validator or a node in the network requests a wait time from an enclave (a trusted function). And simply the leader will be chosen according to the shortest wait time for a particular transaction block by a certain requestor. One function will creates a timer for a transaction block that is guaranteed to have been created by the enclave, while another function, verifies that the timer was created by the enclave. By any chance if it has expired, it will create an attestation that can be used to verify that validator did, in fact, wait the allotted time before claiming the leadership role [24].

2.2.3 Limitations of Blockchains

Limited rules and regulations: Since Blockchains are a rapidly developing new technology there are very few existing laws and regulations that could govern the usage of Blockchains. The novel Blockchain models challenges the existing mechanism for trust by adopting a decentralized authorization mechanism [20]. Due to the lack of laws and regulations the implementing of Blockchains over the borders of countries has become a challenge.

Mining power: as it is explained in the previous chapters the mining capabilities of a particular blockchain will have a direct impact on the users of the Blockchains. Due to the unequal resource distribution the researchers have concerns about some nations have more power over the other in globally implemented Blockchains [20].

2.3. Possible Application areas of Blockchain Technology

Blockchain gained its first entry to the technological field through the launch of the Bitcoin application revolutionizing the digital currency and the financial sector, thereby becoming one of the fastest growing technology with much other potential applicability according to the recent researches and studies [26]. When analyzing the recent researches conducted to explore the potential uses of Blockchains, many have identified and classified these uses into different categories which then can be used for further discussion.

2.3.1 Blockchains in the financial sector

The most popular application of Blockchain technology is in the field of finance due to the assurance it provides of the valued transparency between the trading parties. Blockchain characteristics enable secure, fast and relatively cheap transactions with benefits like fraud detection, crowd funding and decentralization. Provided through the Blockchain technology, many researches and studies have identified the suitability of this technology in the financial sector. The usage of digital currency incorporating Blockchain started with “Bitcoins” which has now spread vastly, creating many other currencies such as Ripple, Litecoin, Darkcoin, Namecoin and Primecoin which uses the Blockchain technology [27][28]. This vast adoption of the technology is leading to a major techno-social upheaval which will reduce the power of traditional institutes which governed the finances like the governments and banks and cause a complete enterprise transformation combined with risk management framework which will enhance the performance. [29][30]. However along with the potential benefits there are possible drawbacks of incorporating Blockchains in to the financial system in terms of legal and regulatory challenges according to the current studies. These can raise considerations in consumer protection mechanisms, controlling the engagements in illegal transactions like tax evasions and trading illegal good and also the law enforcement. [28]

2.3.2 Smart Contracts

As per the definition introduced by Nick Szabo in 1994 for smart contracts still remains broadly useful in the context of Blockchain based Smart contracts where it adopts a more active and an autonomous role in the management and implementation of transactions. [27], [29] The purpose of smart contracts is achieved by embedding the code which contains an agreement between two or more parties, in the Blockchain and allowing the transactions to be automatically self-executed in response if specific conditions are met. This concept can be applied in different sectors to automate the processes like the procedures associated with loans and insurance in the financial sector to assist money exchanges or to automate inheritance, and to carry out ordering in supply chain management [29].

Different developers and researchers have incorporated Bitcoin overlaid protocols to integrate with smart contracts to allow the users to purchase derivatives issuing their own

currency using the Bitcoin network as credit for their exchanges to expand the scope even more [27]. Currently the application of smart contracts has been further supported by independent platforms like Ethereum and Codius which allows users to create virtual contracts for limitless different intentions ranging from commercial purposes, real estate/Own will transfers or to automate betting purposes etc. eliminating the previously needed trusted third party to complete these transactions[27],[29]. However in despite of the advantages, setting up smart contracts still requires initial effort and expense making it more suitable for repetitive agreements rather than one time contracts. Furthermore, researchers have raise their concerns in terms of the efficiency of using smart contracts since they function according to predetermined states and the contracts should not be subjected to major changes during the contract period. Along with the level of legal uncertainty not only it limits the contracts to relatively consensual relationships and agreements which are unlikely to disrupt by the parties it creates the need for the clauses and conditions which trigger the self-automation of the contracts to be in a digital nature suited for digital automation to make the procedure more effective [29].

Blockchain based Smart contracts adopt active and an autonomous role in the management and implementation of transactions [27] [28]. The purpose of smart contracts is achieved by embedding the code which contains an agreement between two or more parties, in the Blockchain and allowing the transactions to be automatically self-executed in response if specific conditions are met. This concept can be applied in different sectors to automate the processes like the procedures associated with loans and insurance in the financial sector to assist money exchanges, real estate transactions or to automate inheritance, and to carry out ordering in supply chain management [28].

2.3.3 Blockchain applications in e-voting

Because of the fraudulent incidents associated with voting procedures reflecting electoral frauds and large absenteeism percentages [27] many countries are now compelled to experiment with e-voting which is considered to be a more promising advancement which can lead to cost and time reduction along with the ability to increase the engagement and the turnout ensuring the secureness of the election procedure. Using Blockchains in the e-voting mechanism is hugely discussed in current researches as Blockchain enabled e-voting (BEV), because of the potential of Blockchains to enhance the security of the systems and to involve more people in the decision-making process through elimination of the power contained by a

central authority. In order to create a BEV system there are two main approaches that can be followed such system as either developing a new bespoke system designed to reflect the specific characteristics of the election and electorate or by using much cheaper and easier established Blockchain [29]. The paper presented by George Foroglou and Anna-Lali Tsilidou named “Further applications of the Blockchain” provided facts about three such project that have been deployed, namely BitCongress, Remotengrity and AgoraVoting which uses platforms like Ethereum and bitcoin networks to generally transforms the system from paper based physical state to a digital system with much more convenience and reliability [27]. With the success of these experimental initiations currently many analysts point out the possibility of using BEV systems to support much more deep transformations like enabling national elections, virtual administrations and 'liquid' democracy [29]. However according to the current researches accessibility and anonymity are two major concerns which arise when implementing a BEV system along with how to ensure and build the trust in the security and the legitimacy provided through the system among the users. Since Blockchain protocol is somewhat complicated for the public to understand the developers of these system not only should concentrate on the accuracy and the security but also to enhance acceptability and the confidence and trust the public has towards these digitized systems.

2.3.4 Managing digital rights, intellectual property rights using Blockchains

Similarly, researchers have also identified the possibility of applying this technology to enforce the protection of intellectual property rights [27]. As suggested through the current studies Blockchain can be used to manage the consumer rights associated with digital products by recording the ownership history of digital property and by even enforcing digital rights thereby protecting both consumers and the creators of the work. By incorporating Blockchains into registering transactions and transfer details of digital artifacts, it allows the users to check the ownership history and determine the legitimate ownership of the content. Using Blockchain as an IP registry can also provide more clarity for the copyright authors, owners and users since it ensures tamper-proof evidence ownership by being a permanent, time-stamped, decentralized, immutable store of information [31]. Any party would be able to view the complete ownership of work including any licenses, sub-licenses and assignments.

Apart from being able to track the ownership, using Blockchains also enable to identify the version of the digital product whether it's the original or a copied version thereby protecting the consumers ensuring that they are not propagating unlicensed copies as well as the creators by allowing them to claim the rights after the sale of their content for example like the royalty fees. According to the predictions by the researches along with law having an important role in identifying and protecting copyrighted work and dispute resolving, with the development of Blockchain can lead to multi-territorial licensing policies and enhanced legal certainty for creators and purchasers along with effective issue resolving ability for digital rights [27]

Currently platforms like Blockai and ascribe [31] have deployed services incorporating Blockchains to allow the authors to obtain a digital certificate of authenticity to prove their work thereby to obtain copyright ownership and to monitor how their work has been used on the internet and for what purposes and to identify and stop infringements and put in place licenses for any use they wish to authorize [32]. When it comes to the issuance of patents two features of Blockchain technology make it particularly relevant to the patent system namely 'hashing' and 'proof of existence' allowing the current patent system to be more efficient through the use of Blockchains [33]. However these implementations associate drawbacks like the threat to the user privacy due to the perfect provenance offered through the registries and the decentralized nature prohibits the removal of unwanted illegal content. It may also limit the "creation" aspect of content if smart contracts and micropayments lead to limits the access only to those who can pay and may be difficult to correct any mistake that was in the original work during the time of entry [31].

2.3.5 Internet of things (IoT)

Many researchers believe Blockchain technology is the key aspect missing from Internet of Things to provide the required trust, record of ownership, transparency, and the decentralized communication backbone much needed for IoT. Because of the better coordination of devices due to the decentralized nature in the Blockchain approach with the features provided through Blockchains like timestamping, smart contracts and encryption. It will eliminate issues like single point of failure and tampering of information and privacy concerns [33] [34].

Under the Internet of things (IOT), different applications of the Blockchain technology referencing the researches done in the domain can be presented, for example like digital tokenized assets transfers, smart contracts, privacy preservation and transaction of smart property, which were also explained in detail in the previous sections [35][36]. By incorporating Blockchains with IoT people will be able to track the history of unique individual devices through the recording of data exchanges that took place between the specific device and the other devices, web services or human users. Using this technology may lead to further leverage the capabilities of these individual devices and convert them into "Smart devices" which can perform as independent agents with the ability of automatically continuing its operations on its own for example like a vehicle diagnosing its maintenance schedule, vehicle registration renewal and do the payments automatically [34]. It will be also useful in the financial and commercial sectors to create IoT enabled devices like remote ATM machines that are able to conduct automatic maintenance and use sensors to conduct property evaluations for real estate management. These IoT solutions can enable secure, trustless messaging between devices in an IoT network and also to further leverage it with the use of smart contracts which then model the agreement between the two parties. Apart from the above mentioned areas another special application is the "Smart property", which is an extension of Internet of Things and the smart contract concept to create an ownership for a physical asset which is controlled via Blockchain [27].

When analyzing the potential of the Blockchains in IoT, a novel possibility that is in discussion is the Decentralized autonomous organizations (DAOs) which can be described as a collection of smart contracts enforced according to a set of governing rules through Blockchains [29]. These networks have the potential to act as independent agents focused on fields like banking and arbitration which were earlier relied on a third party to act as the centralized trusted authority. Examples of such systems can be given as electronic couriers to securely transfer sensitive information, escrow services to transfer ownership rights and even auto-installation services to verify and push updates to the software governing other DAOs [34].

There are possible drawbacks along with the benefits such as Scalability issues and power and time consumption due to the usage of different devices enabled with a variety of computing capabilities. As mentioned in the above section, even this technology eliminated the central authority the decentralized ledger should be stored on the respective nodes which

increases in size with the time. This may be a huge drawback since many smart devices like sensors have very low storage capacity. By widening the use of Blockchain technology with smart devices will raise legal and compliance issues since it's a new territory which is not fully covered by the existing laws creating a challenge for the manufacturers, service providers and respective authorities [33].

2.3.6 Blockchains in Public Services

Blockchain technology can be applied in Public services to enable faster, reliable, secure and transparent delivery of government services to constituents.

Theoretical research done by Marcella Atzori [36] was focused on identifying key features of a Blockchain based e governance system by analyzing the applicability of Blockchain and decentralized solutions for replacing the centralized authorities. Ten main principles of Blockchain-based governance were identified during the study such as centralized organizations and the problem of scale, state as a single point of failure (SPOF), distributed architecture and trust by computation, Systems of direct democracy, Power of individuals and politics by instant atomic interactions, Borderless globalized government services systems of direct democracy and new social contract.

Furthermore, it discusses the technical limitations of decentralizing government services through the Blockchains. The key points highlighted in this section are Security problems and technical weakness of current distributed Blockchains, disadvantages of permissioned, token-less Blockchains for public sector, Government services and the technological imperative of decentralization. Furthermore, this research paper extends its discussion to identify new challenges which are emerging by moving into Blockchains.

One of the most important areas covered in the research paper presented by the European Parliamentary Research services is the use of Blockchains in public service delivery. They have suggested the combination of the two characteristics of time-stamping with digital signature of Blockchains to develop mechanisms that will allow the users to conduct transactions and to create records with less dependent on third party personnel like government officials and lawyers. Researchers have identified the opportunity this will open up, like land registration, marriage registration, patent management, passport issuance and income taxation

systems which might lead to huge improvements in the respective processes after the adoption of Blockchain technology [30]. A Blockchain can become the underlying technology that enhances the accountability at a very local level reducing the reliance on the central governance, promoting the collaboration among the civilians and government organizations. Currently many governmental organizations are at the experimental stage with likely systems. Estonian government experimental initiatives to incorporate Blockchains in different public services like Voting, banking and taxes, welfare payments in the department of Work and Pensions in the United Kingdom and land registration applications in Ghana, Kenya and Nigeria are examples. [29] Using Blockchains in the government services in the commissioning of land title registry by the government of Honduras which records and transfer the ownership of the property and storing the surveyed data regarding by the Connecticut's Department of Economic and Community Development can also be stated as further examples. In addition to enabling these secure public databases, Blockchains will make possible the initiation of novel services like financial reporting or purchasing system based on the Blockchain with the ability of public inspections which could provide assurances to citizens that their public funds are being spent responsibly [36]. These have further proven the benefits that will be received by the users if Blockchain technology is introduced to public administration. However, the risks associated with the initiation of these systems like the set-up costs and the potential technical and procedural difficulties in running backup and parallel systems during transitional phases also needs to be fairly analyzed before deploying a Blockchain based system.

2.4. Blockchain Applications in Public Data Management

2.4.1 Blockchains to manage data

Alongside with the recent developments of Blockchain technology, the researchers all around the world have done researches on adopting Blockchains for public data management. Due to the growing demand for data storage the ability of Blockchains to handle massive data has been questioned.

"Public Sector Innovation Using the Bitcoin Blockchain Technology" done by Svein Ølnes of Vestlandsforsking Western Norway Research Institute is a conceptual research which explored the Bitcoin and Blockchain concepts to propose a model for storing Academic certificates on a Blockchain related to the University of Nicosia. Instead of storing each

individual certificate on the Blockchain, an index document is created containing individual hashes of certificates using SHA-256 and stored on the Blockchain. This will provide a mechanism to verify the certificates through the comparison between the index document and a valid index document from the University of Nicosia. According to the further enhancements presented in the paper, the proposed model can be further extended for the storage of all types of permanent or relatively permanent, public documents including contracts of different types such as procurement contracts, licenses such as driving licenses [37].

Since the researchers have investigated the adaptability of Blockchains for large data repositories. In the research done by Laure A.Linn and Martha B. Koo the researchers have examined the adoptability of Blockchains to protect the critical health related data repositories. [38] In the process of introducing a Blockchain based solution the researchers have attempted to address the scalability and the data privacy concerns related to health data. This research has highlighted the ability of Blockchains to be used as an access control manager. Apart from storing all the data on the Blockchains researchers are suggesting to store critical data on an "off Blockchain data repository" while using the Blockchain as an access control manager. Instead of storing all the data researchers suggest storing unique identifiers of patients along with an encrypted link (pointer) to the health records. And the real medical records will be maintained at the separate data repositories which are called as "Data Lakes". Those health records may vary from formal medical records to health data from mobile applications, wearable sensors etc. Even in Data Lakes the data are encrypted and digitally signed as well. Another research which was done to verify the adaptability of Blockchains on healthcare systems was done by Matthias Mettler. This research specifies some starting points in health sector where the researchers can begin to adopt Blockchains as a starting point. Another similar kind of a research was done by G. Zyskind et al. [39]. With similar to the above mentioned research this research also focuses on developing a Blockchain based model to protect data privacy while maintaining off Blockchain data stores.

Even though above two researches has used data from completely different two domains they were focused on how to manage large scale data repositories. Both of these researches have adopted a common approach to use off Blockchain data repositories to store data; while Blockchains maintaining pointers to the real data. In the research which was done by Kamanashis Biswas and Vallipuram Muthukkumarasamy [40] regarding smart cities they have designed a solution which is directly using the Blockchain as their decentralized database.

With compared to the above mentioned two researches they have tried to store all the data in the Blockchain itself. And it is important to note that this research was done to verify the adoptability of Blockchains in smart cities. So they have answered the scalability problem of Blockchains by directly adopting it as the data repository rather than using the Blockchain as a control mechanism to access data. The research paper provides a comprehensive design for the data management within the Smart City. The design consists of four layers of the system. Namely they are Physical Layer, Communication Layer, Database Layer and the Interface layer. And the researchers suggest using Blockchain in the database layer as a distributed database. This research clearly highlights the capability of Blockchain to act as a distributed ledger alongside with addressing the scalability issues. Since most of the researches were not directly focused on public sector data management; there are researches that are done on privately handled data repositories. Even Though they were focusing of private data repositories those domains areas collect data massively from general public. Since those researches also had to address the scalability concerns, which were originally faced by the public sector service delivery systems.

Bitland [41] is a classic example for that type of a research. This white paper explores the capabilities of implementing nationwide Blockchains across countries in order to manage data related to land titles. Bitland stores land ownership details in a token which called as a cadastral. The cadastrals are stored in blockchain. The main purpose of the Bitland project is to convert the cadastral into a tradable asset. Smart contract concept is used in Bitland where once the owner changed the token is transferred to the new owner. Due to the large amounts of data this research also addresses the scalability concerns while adopting Blockchain as a data store [41].

Blockcerts is an open standard for building apps that issue and verify Blockchain-based official records which may include certificates for cvic records, academic credentials, professional licenses, workforce development. It enable a decentralized, standards-based, recipient-centric ecosystem and trustless verification through Blockchain technologies. The Bitcoin Blockchain acts as the provider of trust, and credentials are tamper-resistant and verification platform. This open standard consist of open-source libraries, tools, and mobile apps where three repositories make up the digital certificates architecture, namely Cert-schema, Cert-issuer and Cert-viewer. Cert-schema describes the data standard for digital certificates where the digital certificate is essentially a JSON file with the necessary fields needed for the

cert-issuer code to place it on the Blockchain. Cert-issuer repository takes a JSON certificate and creates a hash value of the certificate, and issues the certificate by broadcasting a Bitcoin transaction from the issuing institution address to a recipient's address with the hash embedded within the OP_RETURN field. This is an example of an attempt to store non-financial transactions on the Bitcoin Blockchain resulted in bloat of the Bitcoin unspent transaction database (UTXO). Cert-viewer is used to display and verify digital certificates after they have been issued [42], [43].

2.4.2 Blockchains to preserve privacy

Apart from the concerns related to scalability "preserving privacy" is another concern in public data management systems. With the collection of loads amount of data; the collectors usually transform the ownership of the collected data from the users to themselves. So there is no way that the users can get into know how collected data is used or how frequently they are used. In the research done by G. Zyskind et al; [40] they have managed to keep the ownership of the data at the original owner's hand with the use of Blockchain technologies. By applying along with digital signatures they have converted the ownership to the real users. With introducing a compound identity concept, the researchers have ensured that data cannot be collected by mobile apps without the consent of users each and every time. Another research done by Alexander Schaub et al; clearly shows how Blockchains can be effectively used for e-commerce websites in order to develop a trustless privacy-preserving reputation system [44]. The main challenge for those types of reputation systems is that they should be developed in a way that it could preserve the privacy of original voters. The researchers have used of Blockchains and Blind signatures concept to eliminate third party trust issues and enables the voters to express their ideas freely.

2.4.3 Blockchains for authentication

Researchers also have done researches with regard to the adoptability of Blockchains in ownership verification processes as well. In the research which was done by Jeff Herbert and Alan Litchfield; [45] they have tried out to develop a unique Blockchain model in order to address the issues related to Software License validation and verification process. In their approach vendor is represented by his public key while the token includes the details about owner of the software product. This research has highlighted the possibilities of adopting

Blockchains in unique models according to the requirements rather than using the conventional Blockchain model. Even in the BitLand [41] research paper their main focus was to develop a Blockchain based solution that can act as an intermediary between the people who is interested in registering land titles and the officials who are responsible for such public data repositories. With the capabilities of Blockchains the land ownership details verification process has been simplified. Furthermore, in the research paper which was done by Jay Kishigami et al; [46] they have also used the Blockchain technology in order to protect the copyrights issues of digital content. Decentralized peer-to-peer authentication mechanism was used by the researchers in order to ensure the authenticity of a particular digital content.

2.5. Platforms used to build prototypes

There are different platforms available to build blockchain solutions. The mostly used open source platforms are the Multichain [47] and Hyperledger [48].

2.5.1 Multichain

Multichain [47] is an open source software platform that can be used to deploy private Blockchains. The uniqueness of Multichain software platform is that it enables the users to run several Blockchains in parallel. Basic functionalities of a Blockchain such as decentralized nature, time stamping, mining capabilities, asset transactions and permission handling are embedded in the Multichain platform. Hence the users do not have to put an extra effort on establishing those basic Blockchain functionalities. Although Multichain offers the main functionalities capabilities it has its own limitations as well. For instance, users are not allowed to change the predefined block sizes of the blockchain. Furthermore, Multichain initiation and development should be done using command line instructions. However, it should be noted that there are some 3rd party software components which can be used along with Multichain in order to provide graphical user interfaces. Due to the availability of source code the users can customize the platform and use it according to the requirements.

2.5.2 Hyperledger

Hyperledger Composer [48] is a development tool set and framework to develop blockchain applications. Hyperledger Composer is one of the project in the Hyperledger project

group of blockchain applications. In Composer architecture there are 4 components that make the blockchain deployment functional. They are the .cto Model file, .js Script file, .acl Access control file and .qry Query file. The Model file defines all the Assets, Participants and Transaction that eventually take part in the blockchain application. The Script file writes all transactional functions that occur in the application. The ACL file defines the permissions of users to the application. Query file is used to enable queries based on data stored in the blockchain.

2.6. Conclusion

Blockchain technology which emerged with Bitcoin showcases properties which make this technology a suitable database solution to create a data management framework for public data which ensure distribution, data availability and data security. Data management of public data has few prominent issues which cannot be fully eliminated through a typical database solution. Several countries have done few researches to apply Blockchain technology to data management in public service delivery. However, in Sri Lanka there are no significant researches done for the application of Blockchain to data management in public sector or government. Therefore, in the Sri Lankan context there is a research opportunity to analyze the applicability of Blockchains for governance in Sri Lanka and to propose a suitable the framework using Blockchains for public service delivery applications within Sri Lanka.

Chapter 3 - Design

This chapter describes the research methodology that was followed to derive a common framework for enhancing the data management of public service delivery systems in Sri Lanka using Blockchain.

The main focus of our research is to identify the suitability and applicability of Blockchain technology for the Sri Lankan public data management systems context. As for the design phase, an analysis is done regarding the three public service delivery systems that were chosen, to identify the existing issues and design a suitable approach incorporating Blockchain to overcome the identified drawbacks of the existing systems with respect to different centralized/decentralized data management solutions which can be incorporated into the public-sector organizations.

3.1 Research Design

3.1.1 Research Approach

The research process was structured as a six-step process in order to ensure the completeness. Following are the specified six steps which were followed in a sequential order.

1. Studying current Public Data Management Systems and identifying the existing challenges in delivering value to general public

As the initial step of our research we have studied several active public data management systems in order to identify the existing problems. Currently some of the Sri Lankan public data management systems are operating in a transformational phase. Some processes have completely automated while most of the processes are automated partially. Even for the systems which are fully automated the services are delivered both in electronic form as well as in manual form parallel. As it is clearly described in the introduction chapter, Sri Lankan public service delivery systems face a variety of challenges in providing services to general public. The identified main concerns in public service are namely, data accessibility

concerns, data loss concerns, concerns related to frauds and errors, and privacy related concerns.

2. Investigation of the features of blockchain technology to address challenges in public data management systems, which cannot be addressed through current database solutions

In order to find a clear justification for adopting blockchain technology we have done a detailed analysis between different data management solutions such as centralized databases, decentralized databases and Virtual private databases. A comparison between Blockchains and other solutions were done based on four criteria namely, the possibility to manipulate a record and remain undetected, data loss possibility, convenience in providing accessibility and privacy preserving ability. Through the comparison, it is justified that the characteristics of blockchain technology possess the ability to achieve all four criteria.

3. Identifying three public data management systems which would utilize the properties of blockchain technology to create value by resolving issues in their current systems

Among the number of public services available, we decided to choose Birth Marriage Death certificate issuing process [4], Land Title Management, and Health data records management systems to design systems which incorporate Blockchain technology. Reason for the selection was based on the e-government initiatives in world wide. In most of the countries, the first preferred systems for e-government transformation are the Identity management and Birth Marriage Death certificate management, land registry management and health data management. Another main reason behind the selection is that all these processes are accessed by the majority of the Sri Lankans and these were some of the main processes which were focused by the e government initiatives launched by the Information and Communication Technology Agency Sri Lanka (ICTA) [4]. As per the Information and communication Technology agency, major portion of the data relevant to these processes have been converted into digital form and the rest is converting in ongoing projects. Therefore, with consideration to the feasibility of the proposed solution we decided on the above mentioned three processes.

4. Designing of three selected data management systems using blockchain technology

In this phase we designed the overall architecture of the three selected public data management systems to adopt the features in blockchain technology. The objective of the designing was to use blockchain characteristics can be used to address the existing concerns of those particular systems.

5. Designing an abstract guideline/framework by selecting properties from the selected data management systems

The selected systems are redesigned with blockchain to address the concerns which are specific to the particular system. Since the data management processes of different systems are not similar, there are some significant differences between those three designs. At this phase our attempt will focus on generalizing designs of the selected systems to come up with a common data management framework that could be used in government data management systems. As explaining in future sections, at the process of generalization we have focused on six criteria namely, Nature of Blockchain which is suitable for Public Data Management Institutions, Extent of Blockchain usage, Mining, Node involvement, Suitable Infrastructure and Issues and Concerns.

6. Evaluating Abstract Prototypes

Abstract prototypes were developed and evaluated in this phase. The extracted design evaluated based on four main concerns which we have specified in the step 1. Evaluation was a qualitative one based on criteria,

- Possibility of deleting/ modifying a record in the blockchain
- Tracking history of records
- Convenience of accessibility providing
- Preserving privacy of records

In order to develop prototypes; platforms were used because developing a blockchain from scratch takes a huge effort which is not possible within the research time period. Therefore when transforming a data management design into a prototype exactly mapping was not achievable. To develop the prototypes 2 different platforms were used, namely Multichain [47] and Hyperledger Composer [48]. The reason for the selection based on the preference of

blockchain application builders who use blockchain to store digital assets. Most of them preferred Multichain and Hyperledger which are open source platforms. Land Title Management was developed using Hyperledger Composer and eHealth record system was developed using Multichain platform [47]. Hyperledger Composer is a blockchain solution which can be easily adopted to store digital assets with its existing components as explained in section 2.5.2. Therefore, for Land Title Management System it was used. Multichain [47] is ideal for storing chunks of data and flexible to customize as it has a set of APIs that can be connected. Therefore, it is used for eHealth record System.

3.1.2 Limitations to Research Approach

In prototype development 2 platforms used namely Multichain [47] and Hyperledger Composer [48]. However, Hyperledger Composer platform was not flexible to customize to our need to cater the Land Title Management. Even Though Hyperledger is ideal for digital assets, since only the executable is provided, the ability to customize was limited. So, its functionality could be checked only in the storage aspect of blockchain. Mining and accessibility could not be evaluated using that particular platform. Therefore, the evaluation had to be limited to the data manipulation possibility and data loss in the Hyperledger prototype.

3.2 Blockchain Designs

This section of chapter includes the redesigned Data Management Systems using blockchain for public service delivery applications considered.

During the research, when analyzing the processes of data management and literature survey, we found that there are two ways of applying blockchain technology to data management as,

- Storing whole set of data in blockchain
- Storing critical information or hash values of certificates in the blockchain and storing rest of data in a separate database

In order to check the adaptability of the blockchain in public data management systems in Sri Lanka we have selected three main systems, namely they are the

1. Birth, Marriage and Death certificates management
2. Land Title Management
3. eHealth Records Management system

After analyzing those public data management systems, we have designed the systems with the assistance of blockchain in a way that it could address the existing common concerns of those systems.

Accordingly, the selected public data management systems are designed with blockchain as follows

3.2.1 Birth Marriage Death Certificates Management System

The Birth Marriage Death certificates management process (BMD project) [4] that is currently being operated in Sri Lanka is a result of one of the e-government initiatives by ICTA. According to the initiative, the manual process of issuing the copies of Birth, marriage and death certificates was replaced by a single computerized system, which issues the certificates that belong to a certain divisional secretariat of Sri Lanka. However the initial recording of the certificate is still done manually for the first time and the public is issued with a physical copy of the certificate. However in occasions where the citizens are in need of obtaining another copy of their certificate or in case where the certificate they own is damaged or lost they will be able to obtain the service provided by the computerized certificate issuance process at the divisional secretariat. List down below are the phases associated with the current process which is in operation at the district secretariat offices in Sri Lanka.

1. The certificates are recorded by the authorized officers of the government physically, at the point of initiation at the respective institutes relevant to Birth, Marriage, Death certificate issuance and then the "physical documents" will be handed over to the relevant divisional secretariat office once in a six months period by the same authorized officer who issued the certificates as mentioned earlier. The relevant divisional secretariat office will be determined according to the district, division and the provincial area, where the issuance of the Birth, Marriage, Death certificates took place firstly and the period of six months is considered to be a standard time interval to update the details about the newly prepared certificates during that

time period to the BMD project databases at each respective district secretariat offices around Sri Lanka.

2. The physical documents which are being collected by the data entry operator in the relevant divisional secretariat office, will then be scanned and stored in a database located at the local government institute along with the user critical data specific to each certificate for retrieval purposes. The user critical data will be entered by the data entry operator at the point of uploading the scanned images of certificates, which is same for all the procedures associated with Birth, Marriage, Death certificates. The data entered as "user critical data" is common to the three types of certificates handle by the system, and the respective data fields are mentioned below.

User critical data for Birth, Marriage, Death certificates

1. Document Type (Certificate Category) - Whether the particular certificate which is being uploaded to the system in a Birth, Death or a Marriage certificate
2. District Secretariat - Name of the District Secretariat office applicable for a particular certificate (Any Birth, Death or a Marriage certificate)
   Example - Kesbawa
3. Division - Name of the Division applicable for a particular certificate (Birth, Death or a Marriage certificate)
   Example - Sri Jayawardenapura
4. Name- Name of the Certificate Holder
5. Name 2 - Names of other respective people mentioned in certificate
   Example - A parent name mentioned in the Birth Certificate
   Spouse Name on Marriage certificate
6. Date - Value for the date field mentioned in each certificate type.
   Example - Birth date in the Birth Certificate
7. Serial Number- Serial number for the respective scanned image which is uploaded to the database which is usually system generated.

3. In terms of the certificate retrieval procedure, public is able to obtain the copy of the necessary certificate (Any Birth, Death or a Marriage certificate) by visiting the relevant divisional secretariat that they belong, based on the location where the certificate was initiated.

And the requestor of a certificate have to pay a fee of Rs. 100.00 per certificate and obtain a receipt from the local government institute before going to the operator to retrieve the document as a prerequisite.

4. After obtaining a receipt of the payment, In order to retrieve the scanned image of the certificate document, which is done by an operator in the respective district secretariat, the individual who is in need of a copy of the certificate should provide the details for the "user critical data fields" (Information for a particular number of search fields based on the critical data entered to the system by the data entry operator in the above step).

5. The operator at the local government institute will be able to search for the relevant certificates type based on the data provided by the requestor and the search results will vary depending on the amount of information provided for the search. Finally the retrieved documents will be shown to the requestor, to select their own certificate, and the operator will provide a printout of the selected certificate.

Illustration of the current system

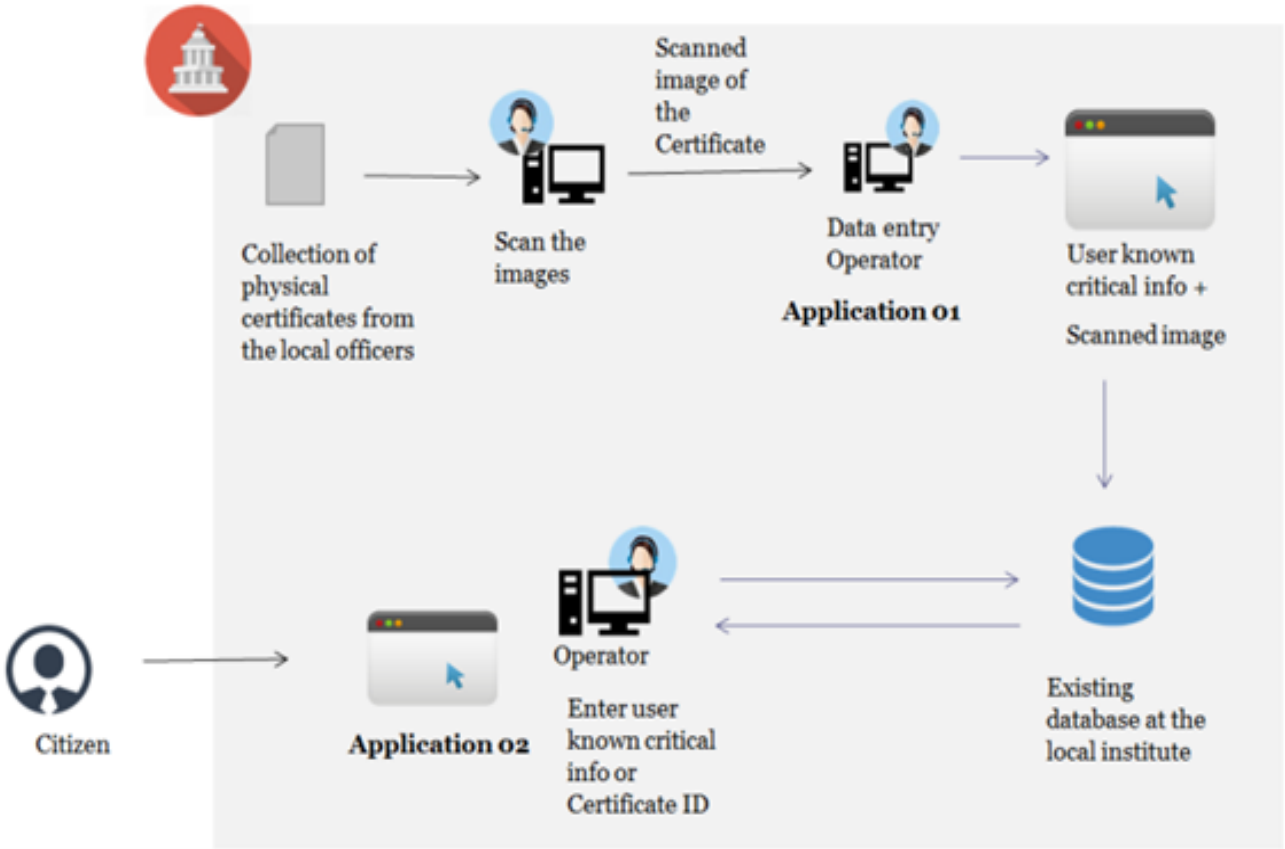


Figure 2- High Level Architecture of the current BMD Certificate Management System

Some of the screens from the actual BMD project is shown below.

1. Initial screens for the search function of the certificates are shown below. From the field "Document type" the operator will be able to select which type of certificate that is being requested.

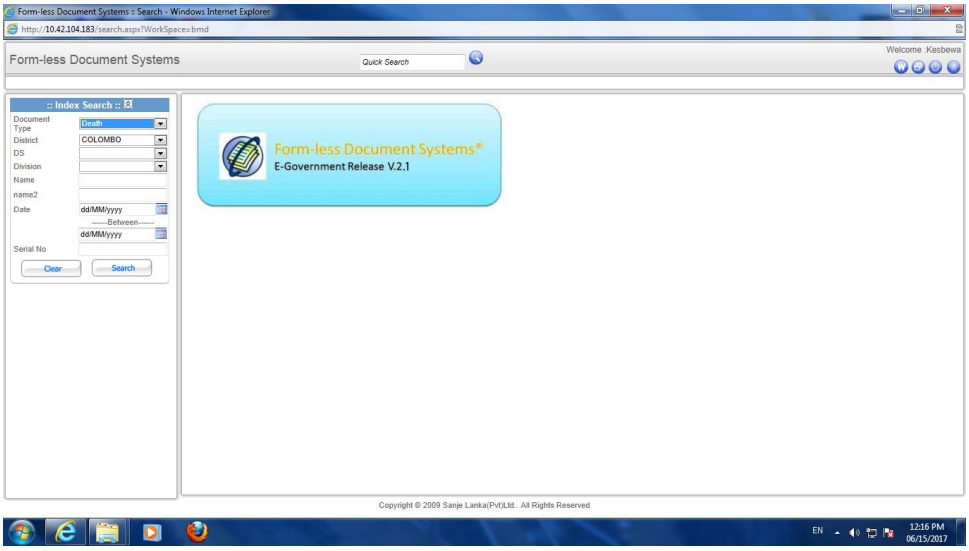


Figure 3- Initial Search Screen of the current BMD System1

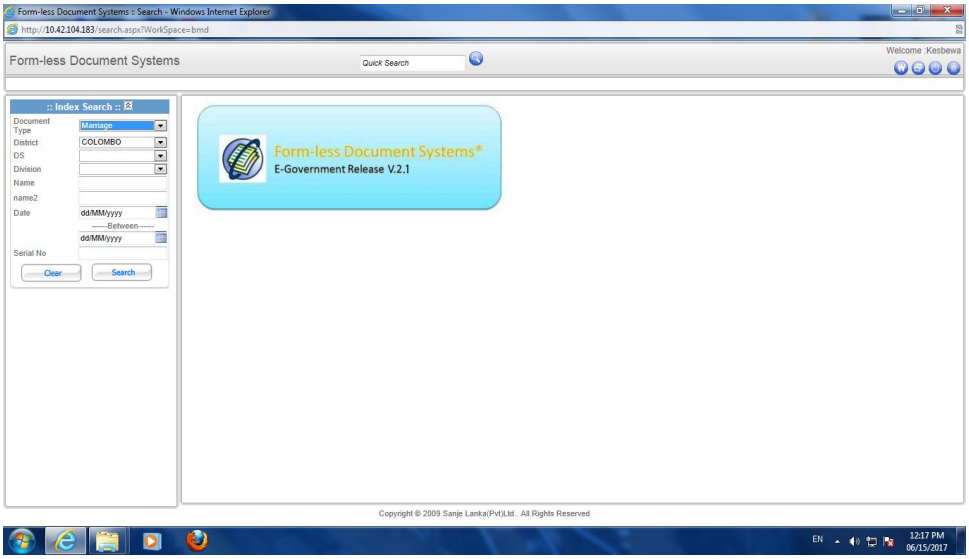


Figure 4 - Initial Search Screen of the current BMD system2

2. The search result screen after the operator fill the search fields according to the input of the requestor. In the below scenario, since information for all the fields are given, only the certificate with the relevant details are shown. The operator then can approve the print of the certificate after viewing the scanned image of the certificate.

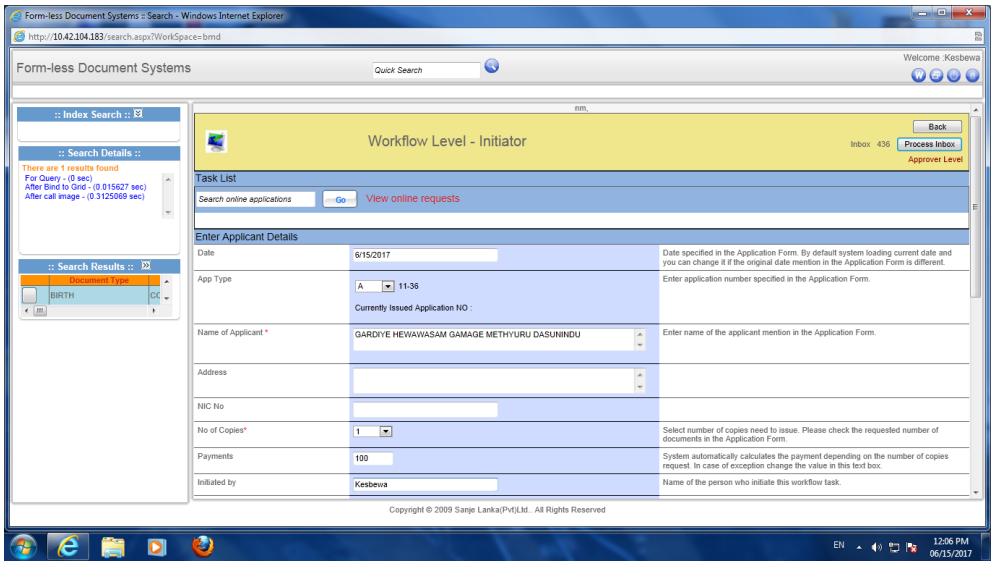


Figure 5- Search result screen for a specific search query for a particular certificate – 1

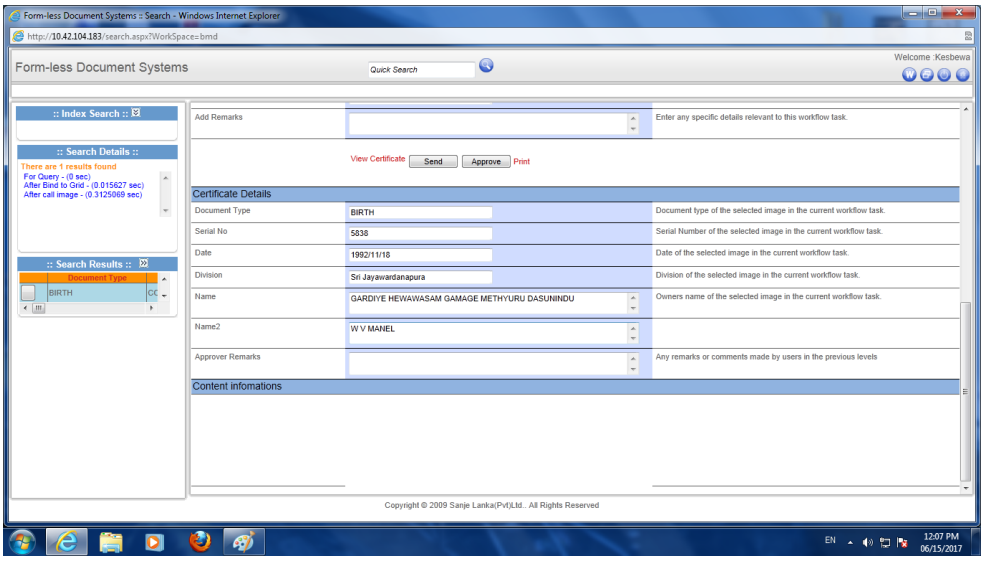


Figure 6- Search result screen for a specific search query for a particular certificate -2

Issues with the current process

- Isolated databases at each divisional secretariat office restricting the access of information

According to the current system, the scanned images of the certificates of a particular divisional secretariat will be residing in their own database situated at the local premise. Therefore, if an individual need to obtain a particular certificate irrespective of whether it's a Birth, Death or a Marriage certificate, must visit the divisional secretariat which owns that certificate according to the location of physical initiation of that certificate in the first place. For example, if a person is living in Colombo and that person's birth location is Jaffna where his/her Birth certification took place, he still needs to travel to that particular divisional secretariat to obtain a copy of the Birth Certificate if a need arises. Because whenever a verification is needed for a particular certificate (Birth, Marriage or Death Certificate) for different purposes, for example obtaining a passport, for employment related activities it's purely based on the sealed physical documents. Therefore, public face a difficulty cause there is no alternative way other than traveling to the divisional secretariat where their certificates resides.

- Risk of data loss

Since the certificate information belongs to a particular Divisional secretariat is residing in the local premise in their own database, there is a risk of losing data if a corruption in the database occurs or in case of a natural disaster. Since the cost and effort incurred in scanning the certificates and entering the user critical data is a considerably high it's important to have a backup of the data which will be again associated with a certain cost.

- Recovery of the scanned images and data in case of a failure

As mentioned in the earlier point, in case of a failure in the databases according to the current system the recovery should be based on a backup which is also residing at the local premise which might be subjected to the same failure or a natural disaster if any case. Then the recovery might be based on the physical certificates maintained in the premises which is also face the possibility of getting easily damaged. Since there is no backup maintained in elsewhere other than the local premises there is a concern on a fully effective recovery in case of a failure.

- Difficulty to identify any change for the documents in the database

When considering the current system, the certificates are stored in the form of scanned documents. And since this information are residing on a locally situated database, through any person at the local government institute who has the access to the information in the database will be able to replace any image with a fraud scanned document of a modified certificate and use that as the original certificate without any alarm. If by any chance, a scenario like this took place and the fake document is issued by the respective district secretariat it will be considered as a legal document since the verification will be based on the sealed physical document, as mentioned above.

- Mobility of the document

In here, mobility of the document concerns the fact of the necessity of carrying the physical document of a certificate (Birth, Marriage, Death certificate) for any place for the purpose verification of details about a particular individual. Sometime these certificates will get misplaced, damaged or most importantly this will create the possibility of being able to use a fake certificate as the original document. Therefore, it's important that these document are in a form which is accessible and convenient for the public to carry around and to use in any case of verification of details, and a mechanism to check against the system whether the document is original.

- Verifiability and authenticity of using a physical document as proof

Even Though through the BMD project they maintain a database of the original scanned documents of certificates, institutes which need to check the validity of the respective certificates for different purposes like Banks, Immigration department, Insurance companies does not have a mechanism to verify against those digital information, rather than relying on the physical documents which is being given to them by a certain individual. And in case of a scenario mentioned in earlier bullet points, where the scanned document in the database itself is replaced by a faked certificate and issued by the respective local government authority, the ability to recognize that it is a fraud document will be far more less. Therefore, there is a need to have a proper form of these certificates to get verified without consuming much time and in a reliable way rather than depending on the physical document only.

3.2.1.1 Proposed Design ·

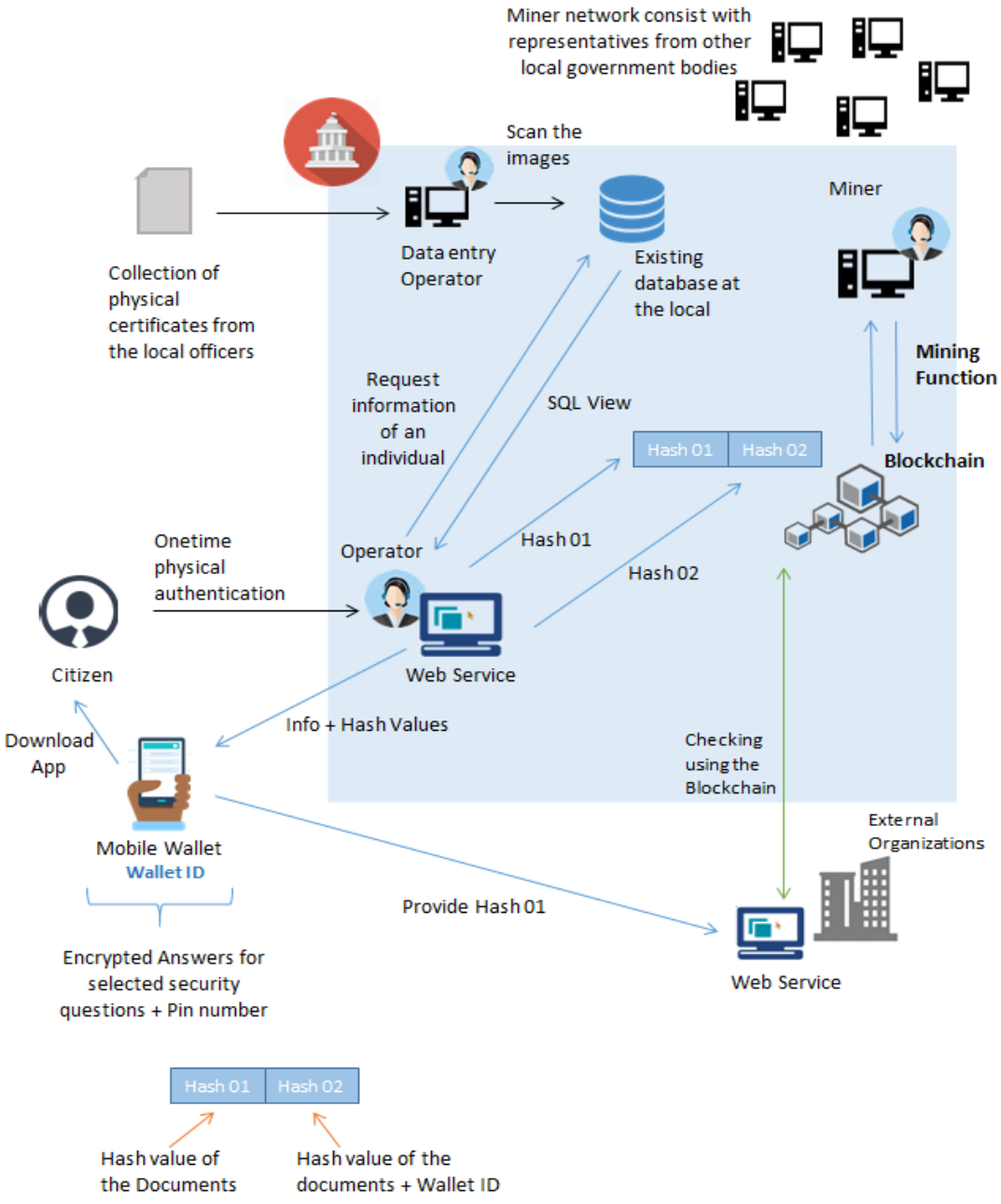


Figure 7- High Level Architecture of Proposed System

As explained in the above section with the issues identified in the current process with relevant to the Birth, Marriage, Death certificate digitalization and management in Sri Lanka, we thought of suggesting a mechanism which will use Blockchains in a way that will be an enhanced mechanism to the existing system which will address and mitigate the concerns arising through the issues. The proposed design incorporate the existing system and its structures as well, along with a blockchain and a wallet based approach to individual citizens.

As in the current system, the solution is common to all the three different types of certificates that is being managed under the BMD project, since we have used the existing system as the foundation of the proposed design. In the proposed design, the issues and the inconveniences faced by the public as mentioned in the above section is considered and is focused on providing a value-added service to the public. In the context of value added service, a blockchain will be implemented to store the hash values of the digital documents and act as a mechanism which allow the third parties to verify the certificates without needing a physical documents as proof. This also has been used in the design to eliminate unauthorized modifications to the scanned images residing in the database and to identify when such instance occur. The blockchain concept in the design supports the mobile wallet concept used in the design to create more value addition to the users with relevant to the certificate obtaining procedure, by acting as a security enhancement which will ensure the reliability and the effectiveness of the wallet functionality and the purpose in the design.

We have proposed a design with a mobile wallet to eliminate the need to visit the divisional secretariat office whenever a copy of the certificate is needed, apart from the first time where the user need to validate the mobile application which is described in detail in the below sections. And according to the discussions we had with the representatives from ICTA as well as divisional secretariat offices, [49] since they have a plan to connect the isolated databases at each district secretariat offices in the near future, the need to travel to the exact district secretariat office for the verification of the mobile wallet will also be eliminated. Since we wanted to design a solution based on the existing system we considered the future implementation plans by the ICTA for this particular BMD project in order increase the actual capability of including the proposed design of ours in a future enhancement to the currently existing system. Even in case of failure to implement the future enhancements by ICTA which is mentioned above through our proposed design the user will only needs to visit the district secretariat once and use the mobile wallet thereafter for the verification purpose of his details.

A mobile wallet in the sense is actually a mobile application which includes the scanned images of Birth, Marriage and Death certificates as requested by an individual at the point of registering the mobile wallet as proposed in the design. The term Mobile wallet [50] is usually used to introduce a mobile application which is used to store credit card or debit card information in a digital form on a mobile device, instead of using physical plastic cards to make purchases, which will actually a replacement for the physical wallet which we carry with us in

day today life and replace it with mobile phone or a smart device which has become an essential need according our lifestyle. Likewise, since the mobile application that is being suggested in our proposed design is a replacement for carrying around and owning physical documentation of certificates for verification with digital forms of certifications with the capability to check the validity we thought of using the term “mobile wallet” in our solution perspective as well. This will ensure the mobility of the documents as well as the identification of any changes to documents in the database without any authorization from the user, as well as acting like a backup for the personal digital documents in case if there is a data loss occurred in the local government body. The proposed design is further explained in the below sections with regards to the processes associated with the system.

3.2.1.1.1 Image scanning process

This phase of the process is already existing in the currently implemented BMD project, which is being carried out by the data operating officer at each divisional secretariat office. The main reason for not changing the existing process is due to the well-established nature of the current mechanism of converting the physical documents to the digital form and it’s located in a database at a government authority. We did not consider to have a digital version of the certificate solely with the user because for validation purposes third party organizations are relying on a centralized authority, which is the government play the validating authority for legal purposes. Therefore instead, the proposed solution is designed in a way that is using these scanned images of the certificates in the database, for the user’s mobile devices as well which are being transferred to the mobile device at the point of registration which is explained in detail in the following steps. Even Though blockchain concept can be used as a database, in our design the existing databases will be used to store the actual images of the certificates. One of the reason behind this decision is the limitation we came across with regard to the storage capacity of a single record in the blockchain database as well as the nature of the certificate, certificate creation and the time period when a specific individual is starting use these certificates for verification purposes.

Furthermore, the intention of our Blockchain based approach is to explore ways we can incorporate the technology and adapt Blockchain in a way that it will overcome the above mentioned issues reflect in the currently implemented solution not just to showcase Blockchain as a database solution. And as mentioned in the earlier chapters, one of the solutions provided

in the global context in terms of Blockchain based approached is the use of smart contracts [29], which is a digital creation of a certificate without producing a physical certificate at all using a smart device. However, in our scenario, we did not adapt that design approach because the nature of the certificates that we are dealing with in this particular situation. For example, birth certificate is something which will be created at the birth of a person and it will be remained in the databases of the government authorities until that person is being able to use it as a verification of his own personal details in some later years for different purposes like his employment, obtaining of a passport. Therefore, we designed the system in a way that the users can decide whether they want to obtain the blockchain based mobile wallet mechanism as a value addition for their interaction with these public service providing authorities.

3.2.1.1.2 Downloading and setting up the mobile wallet

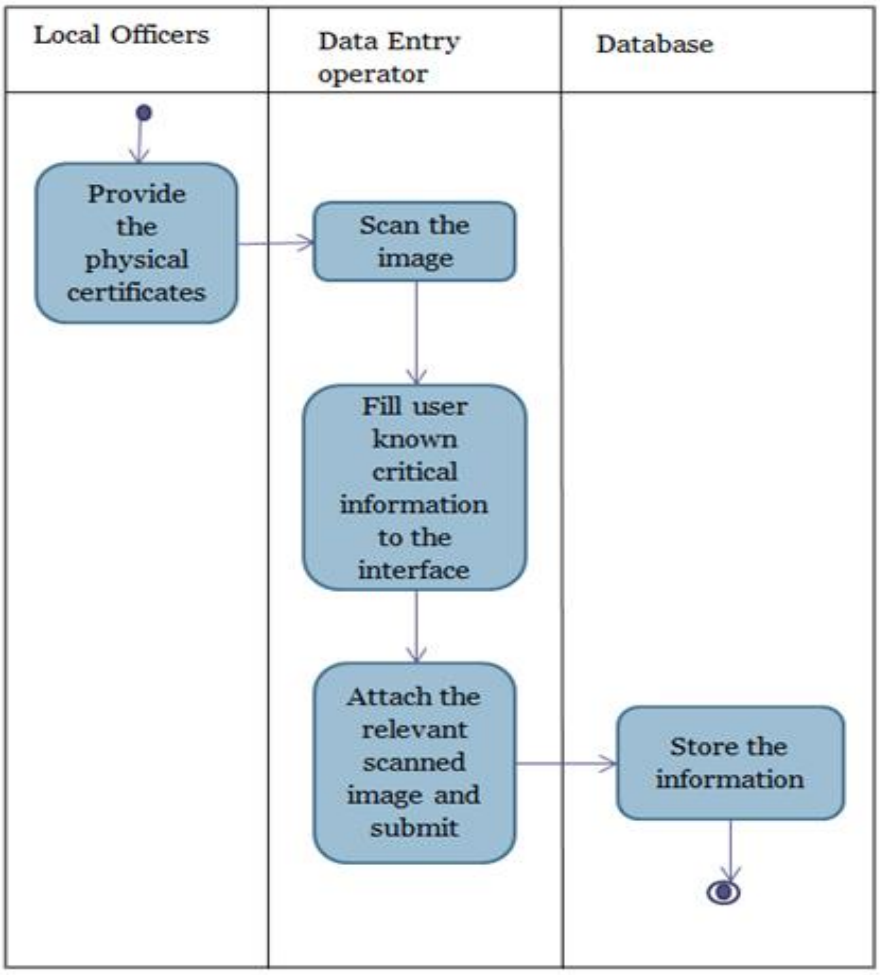


Figure 8- Activity diagram for image scanning process

According to our design if the users wants to obtain a mobile wallet to maintain their own certificates with themselves as well as to use them in verifying their personal information in different scenarios, they are able to download the mobile wallet/application from the app store, which is suggested to be developed for the BMD project according to our design. The user then has to setup the mobile application by providing a PIN number and several onetime answers for a specific set of security questions which are then used to create the wallet ID. Wallet ID will be the unique value or the number which is used to differentiate each mobile wallet owned by different users of the system. Here the wallet ID will be stored within the device. And the reason why it is not a random number is to make it easy for the recovery of the wallet in case of losing the mobile device containing the mobile wallet. Since hash values of the certificates are stored in the blockchain with relevant to the wallet ID, which is used for the verification purposes the users should have the ability to recover the same wallet ID. Recovery of the wallet won't replace the content once recovered and it should be done via following the same procedure of registration of the mobile wallet. If the user doesn't remember the answers for the security questions and the pin number have to follow the same procedure as well, and the existing record of hash values with relevant to the previous wallet ID will be flagged by the operator at the local district secretariat office.

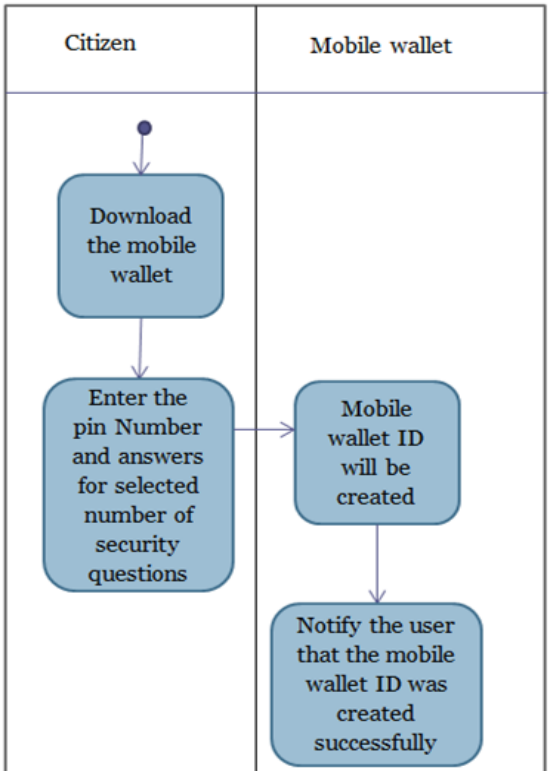


Figure 9- Activity diagram for downloading and setting up the mobile wallet

3.2.1.1.3 Physical Authentication and the creation of Hash

As mentioned in 1.0 since the verification of theses digital documents need the association of a government authority and because the user need to transfer the digital scanned documents of the certificate from the district secretariat office database to their own mobile device an individual in need of obtaining the wallet based service he is required to go to the relevant divisional secretariat office only once to set up the mobile wallet after downloading and doing the initial setup. As an additional step, physical authentication was introduced to the process since there is a need to correctly identify the person and to make sure he/she is the real owner of the certificates which is about to get transferred to their mobile device . An individual needs to present physical verification details in order to correctly identify before setting up the wallet and these details may include the individual's National Identity Card, Passport or else the driving license. And the operator at the divisional secretariat will be able to compare the details provided to him by the citizen and the search result provided by the system.

This search result will be obtained using the currently existing BMD project which is being explained under the current process in the above section which is carried out by obtaining information to fill out the critical data fields in which is in the search functionality. This will further prevent any modifications or frauds that might happen if the operator misuse his privileges. And it's also important that the operator check whether the record is already being associated with a wallet or not before continuing. If the record is already associated with a wallet, it means the citizen has come again for the registration of a new mobile wallet after losing the previous mobile wallet or it's an attempt to fraudulently obtain someone else's information. The operator can re-register the person if that is the case or take legal action in case of a fraud.

After that the operator can create the hash value of the digital certificate he obtained through the search result.

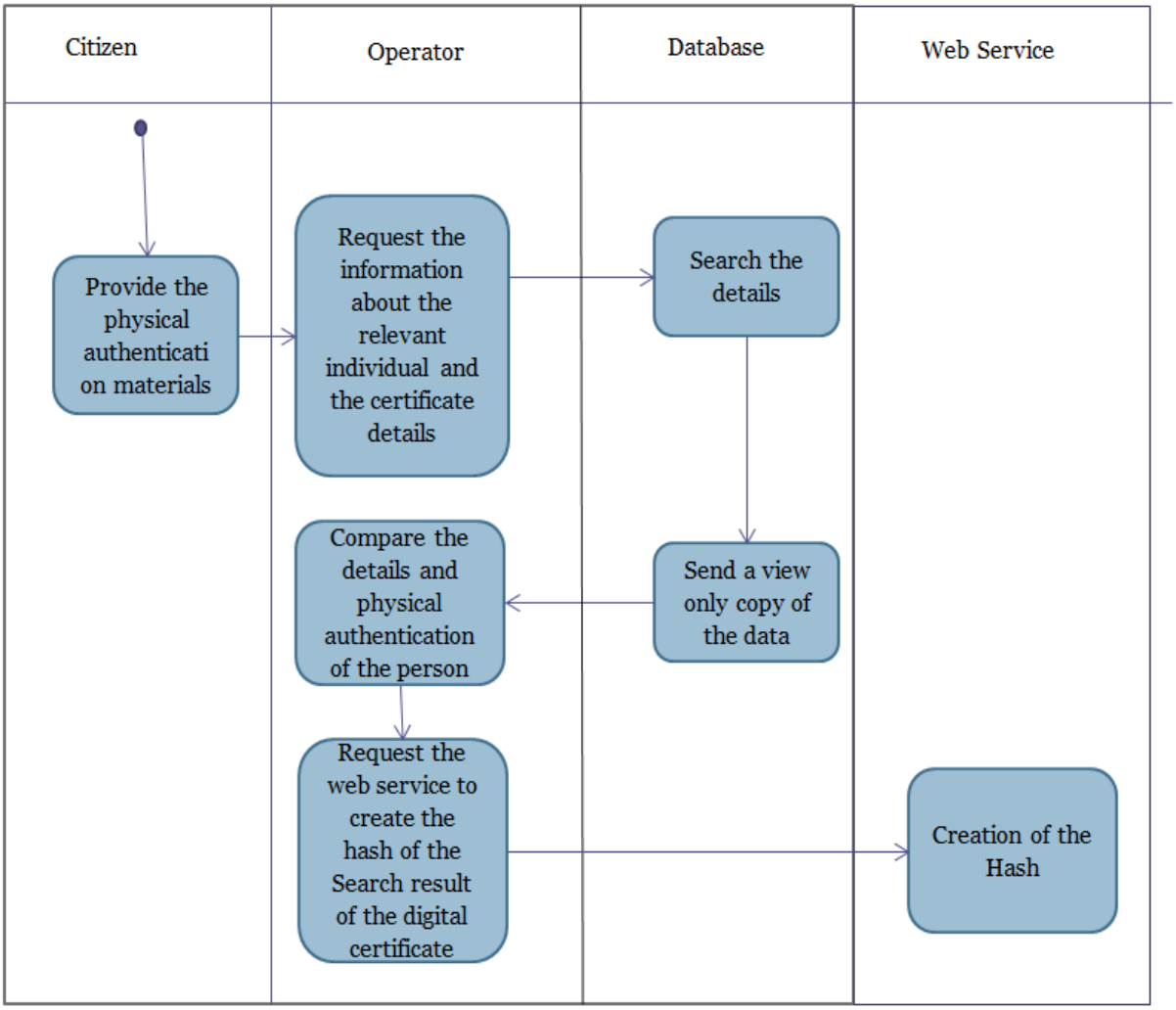


Figure 10- Activity diagram for physical Authentication and the creation of Hash

3.2.1.1.4 Setting up the content

After the user get physically authenticated as the correct owner of the digital certificates he/she is requesting the operator at the district secretariat office can request the user to send the mobile wallet ID to the operator's web service in order to carry out the transferring of the digital certificate details from the local government authorities' database to the users mobile device. As mentioned earlier Hash 1 will be the hash value of the digital certificate document and the Hash 2 is the hash value generated using combining the Hash 1 value and the Wallet ID the user sent to the operator's web service. And here these hashes will generate for each certificate that the user is requesting. The reason for obtaining two hashes is because of the need to bind the right owner with the right verified document with the use of wallet ID owned by that particular individual. And even if somebody is able to generate the hash of the scanned image since it's available in the local database, they won't be able to prove the certificate is an

authenticated one without knowing the wallet ID. Because in our proposed design the certificate verification capability provided to the third-party organizations are done using the transaction that will be recorded in the Blockchain using the two hash values. As mentioned in the above activity diagram a record in the blockchain will contain the Hash 2 value as the transaction ID and the value of Hash 1 as the transaction value.

There will be no issues arise regarding the generation of different transactions for each certificate type from the same wallet because the value of the transaction ID differs even it's created for the same Wallet ID, since the Hash 2 value contain both Wallet ID and the Hash 1 value which is the hash value of the certificate. The process recording the Blockchain transaction involve mining which is explained in detail in the section 2.2.2, and in order to carry out the mining there will be a miner at each of the district secretariat office around Sri Lanka which will collectively for a miner network for the Blockchain proposed in the system. A mining process which is similar to Bitcoin [7] network is not suitable here since there won't be any compensation mechanism involved in the mining protocol as such in the Bitcoin network. Therefore, it will be simply a proof of work based mining protocol [25] where the mining process is based on generating the nonce value which allow a particular block to achieve a block hash value in the format defined in the genesis block [21] of the implemented blockchain. The two hash values will be sent to the user's mobile device along with the digital certificate transferring. The blockchain which is proposed to implement in the design is a private blockchain in the sense the mining will be done by some allocated miners in each respective government organization, but it is opened to access and view the transaction by authorized third party organizations to carry out the verification of digital scanned images if certificates presented to them by the citizens.

Web portals can be created for institutes like banks or other government bodies to access the blockchain, by searching through the transaction ID provided by the citizen through the wallet which is the Hash 2 value. Verification can be done by comparing the Hash 1 stored in the wallet and the Hash 1 value in the particular search result of Blockchain transaction.

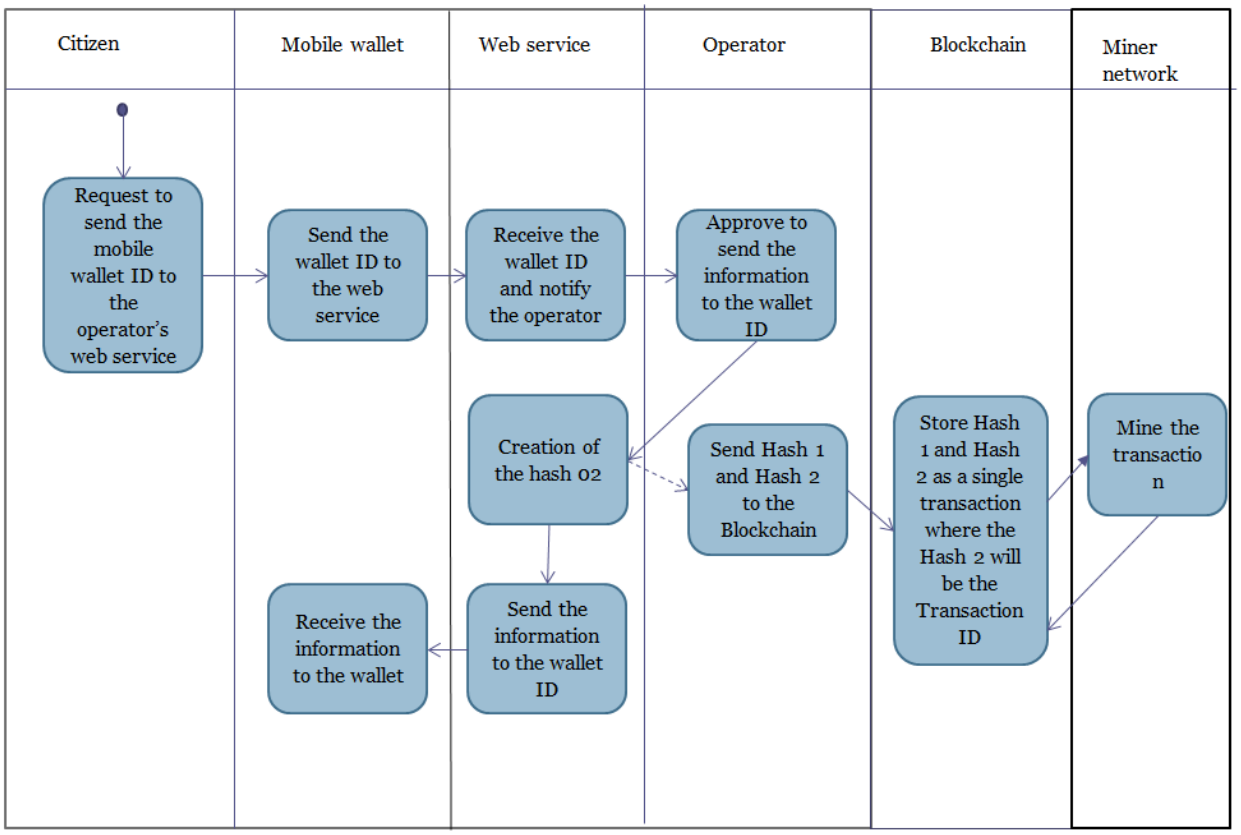


Figure 11- Activity diagram for setting up the content

3.2.1.2 Designed block structure for a block in Birth, Marriage, Death Certificate Management system

Block No: 128

Block hash: 00007835419b4ba8e8faeb6d2f08d4ba70fffdeed4f1fd2d99ca546107f54326

Nonce value: 47834298

No of records: 6

Timestamp: 1501432977

Mined by: Colombo

Previous Block: 0000c2d4bd9d75caa90aa7a08fda901cbca7bcfa3443a1eb3b52325d730b8897

Merkel root: 3BA3EDFD7A7B12B27AC72C3E67768F617FC81BC3888A51323A9FB8AA4B1E5E4A

Block height: 350

Records

Transaction ID - Hash 2 (Hash 1 + Wallet ID)	Hash 1

Figure 12- Designed block structure for a block in BMD Certificate Management system

3.2.1.3 Evaluation of the Blockchain Design

When designing the system for Birth, Marriage, Death certificate management, the 1st phase of designing involved a design that used Blockchain as the sole database for storing the digital version of the certificates itself, rather than using a separate normal database for storing the digital documents. But with that particular design we were able to identify some limitations of Blockchains, which is the storage capacity of a particular block [22]. Since the scanned image of a particular digital certificate is about several kB in size including it in a block as a transaction aroused many concerns with the mining function with relevant to the mining effort, cost and time taken to complete the mining process of a particular block since the normal block size is around 1MB. We were not able to compromise on the size of the image since the quality of the image needed to be considerably high since it will be printed out in order to give a copy of the certificate to any requesting individual. Even Though there is a limitation of using Blockchain as the only database for providing a solution to the system, in the next design phases we were able to incorporate Blockchain as an additional mechanism to the currently existing system as an enhancement to the issues related to the verifiability, security and the mobility of the digital Birth, Marriage, Death Certificates stored in the currently deployed system by incorporating the mobile wallet concept as a supporting concept. Through the design the inconveniences occurring to the users to visit district secretariat office in need of a copy of the certificate or carrying the physical documents as proof for verification purposes will be mitigated. The proposed design also contributes to the security aspect of the process by eliminating the possibilities of fraudulent modifications to the digital data stored in the databases which are either carried out with or without the acknowledgement of the owner of the digital certificates. Since Hash values will be stored in the Blockchain database once the user registers the mobile wallet, since it's append only nobody will gain the ability to modify the digitally stored scanned copies of certificates, since it will be visible through the comparison of hash values of the original document which is stored in the database and the hash value of the fraudulent document.

And also in case the data residing in the local government database got destroyed since the user has the digital version of his certificates with him, the issues that might have faced by him will get mitigate and this copy of data can also be used as backup of the information residing in the local government body. And as mentioned above through the design a solution

to increase the mobility of the document is given by associating the mobile wallet concept and again using the Blockchain to create the acceptance and the reliability of information included in a particular user's mobile wallet. Since through the design we focused on providing a web portal for the third-party organizations the citizens are able to directly use the documents stored in the mobile device in case of a necessity and even obtain a physical copy of the certificate by simply printing the scanned document on the mobile device. And the third-party organizations are also having the convenience of correctly verifying the individual that they are about to provide the service and eliminating the risk of involving or facing a fraudulent action and also by not involving in huge documentation procedure incurring a huge amount of time.

One of the limitations of the current design is that since the mechanism is introduced on top of the existing system of the BMD project as an optional enhancement mechanism, whether the users will be engaged with the mechanism. However, since from the proposed design, the ability to conduct fraudulent actions and to present fraudulent certifications is hugely mitigated we can expect that the third parties involved in different domains will request for this verification service provided through the web portals to access the government's blockchain which will drive the individual citizens to adopt this enhancement. And since in the design phase we focused on the actual applicability of this design to implement this in reality, we had concerns on using mobile wallets or in other words mobile applications to make this service available because of the number of smart devices or mobile devices available among the citizens. But with the huge popularity and the wide usage of smartphones in the future it won't be a concern if we actually deployed it.

3.2.2 Land Title Management System

Land Registry Department provides a particular set of services as registering a particular land under the name of owner, once the deed is registered and issuing copies of stored certificates at request [51].

In Sri Lanka when the ownership of a land is transferred to a new user a new deed document is written in front of a notary in the presence of witnesses. A deed will hold details of the land being transferred and the notary's details including

- Deed No
- Date of deed
- Name of Notary
- Registration stamp duty
- Land details
- Witnesses

When such registered deed is brought into a land registrar department office, the registration of that land for the new owner is done. Request for a registration is done using the deed and an application issued by the Land Registry Department. Application will consist of following details

- Name of Notary who registered the deed
- No of Notary (identifier for a Notary)
- Certified Date of land
- No of pieces are registering
- Previous registration details (if any)
- Value of deed
- Stamp duty
- Stamp duty paid date
- Signature of Notary with Date

Folio records are the documents that holds the ownership details for a particular land. Folio records are created with the details of a deed and some registration process related data.

The process of writing a folio record is considered as the registration of a land title. Registration clerk is the person who does registration and there is a specific clerk for a particular court division. The unique identifier for a particular registration is the Daybook No. The Daybook No is generated in the order of registrations starting from the January 1st for a particular year. Details included in a folio record as follows

- Division of the land location
- Folio No(All registrations for one land block goes under one folio No)
- Name of Land
- Plan No and Date
- Name of Surveyor
- Land Lot No(Specific number that identifies the land)
- Village or town that the land is in
- Pattu and Korale of land
- DayBook No
- Grantors
- Grantees
- Specific remarks(if there are giving up ownership deed is present)
- District
- Province
- Boundaries of land
- No and Date of Deed
- Name of Notary
- Registration Stamp duty
- Signature of Registrar who authorized the registration

There are different roles in the Land Registry with specific set of duties

- Counter- Enters the data in the application+ deed to proceed with registration and forward documents to Assistant Registrar
- Assistant Registrar- Divide deed documents to the relevant Registration Clerk of the court division where the land located
- Registration Clerk- Write a folio record to register a land under the owner's name
- Registrar- Authorize the registration

eLand Registry is the computerized land title management system developed under e-government initiatives. Centralized database is used with a single server and all registration data stored in that server.

1. Registration Process

The usual registration process takes place in a Land Registry Department according to the current eLand Registry system as follows

1. A citizen handover the deed with the filled application form to the counter
2. For the deed to be registered, a daybook No is issued at the counter which is called as the RRRN No
3. The data entry operator at counter enter deed data into the database and forward to Assistant Registrar
4. The Assistant Registrar divides the deeds according to the court divisions and assign them to relevant Registration Clerks
5. The Registration Clerk checks previous folio records and write the new folio to register
6. Acquiring Registrar's approval for the registered deed
7. Scanned copy of the deed is stored in a separate table in the database and the deed document is given to citizen

2. Document Retrieval

When a citizen requests a copy of a Deed or a Folio stored in Land Registry Office

1. Citizen handover application with required details to locate Deed or Folio
2. Operator query the database using provided details and provide a copy

3. Viewing certificates stored at Land Registry Office

In order to verify the integrity of a certificate, requester should be physically present in the particular land Registry Office where the property was registered.

Identified issues in eLand Registry

From the four types of data management issues stated in section 1.2 considered in the research, the eLand Registry is most affected by the data manipulation. If data modified and remains

undetected, integrity of land titles is lost. Since centralized database is used, if data gets deleted data loss can occur if proper backups are not kept. Real time verification of Deeds or Folio is not there.

3.2.2.1 Redesigned System using Blockchain

Using Blockchain properties the identified issues can be suppressed. When Blockchain is incorporated with the Land Title Management, the processes will be as follows. Only a segment of folio data is entered into blockchain. The data that holds the ownership for a land block is entered into blockchain while rest of data inserted into folio table in database. A temporary table is used to carry that data up to the registration and once that data is entered to the blockchain, they get flushed from temporary table. Once a registration is complete, critical data that holds ownership details will be with blockchain and rest of data will be in the database. The blockchain transaction ID which generates when the data entered to blockchain is used as the common key between the database table and blockchain. Validation of data that is entered into the blockchain is done in the registration process itself and the validation completes with the Registrar's approval.

Private Permissive Blockchain is used because the Land Registrar should have the authority of registrations. Customized block structure containing ownership details for a land is used for the blockchain and dedicated mining is done using a pool of miners representing the Land Registry offices.

Public blockchain like Bitcoin cannot be used as the blockchain because compensatory mining cannot be done because the folio record added to the blockchain does not have a monetary value and the mining should be under the control of the Land Registry protocols. Bitcoin block structure is designed to store financial transactions. So that structure does not match for the purpose of storing a digital asset.

3.2.2.1.1 Registration Process

When the Deed is handed over to the Counter along with the Application for Registration of Deed,

- Data is entered to the local SQL Database
- Issue a RRRN No (Day Book No) for the registration
- Deeds to be registered are forwarded to Assistant Registrar

The Assistant Registrar,

- Divide the Deeds to the relevant Registration Clerk

The Registration Clerk,

- Check folio records in the Blockchain for the history of Registration of Land Block
- Register the Deed
- Forward the Registered Deed for Registrar Approval

On receipt of approval, the Registration Clerk

- Enter critical Folio Data to the Blockchain

Blockchain token will comprise of

- Day book No(RRN_No) – unique identifier
- Folio
- Deed No
- Lot No
- Grantors and Grantees
- Hash value of Deed
- Signature of Registration clerk

After adding a particular folio record to the blockchain, a unique blockchain transactionID is generated. It is used as the link between database and blockchain. When the data entered into Blockchain, the pool of miners which represent the Department of Registrar General

- Mine and add blocks to the Blockchain

When the block is added, rest of folio data is submitted into database along with the scanned copy of deed and blockchain transactionID.

Once the Registrar authorize the Submitted transaction

- Deed is returned to citizen along with the blockchain transaction ID which can be used as a reference number to query.

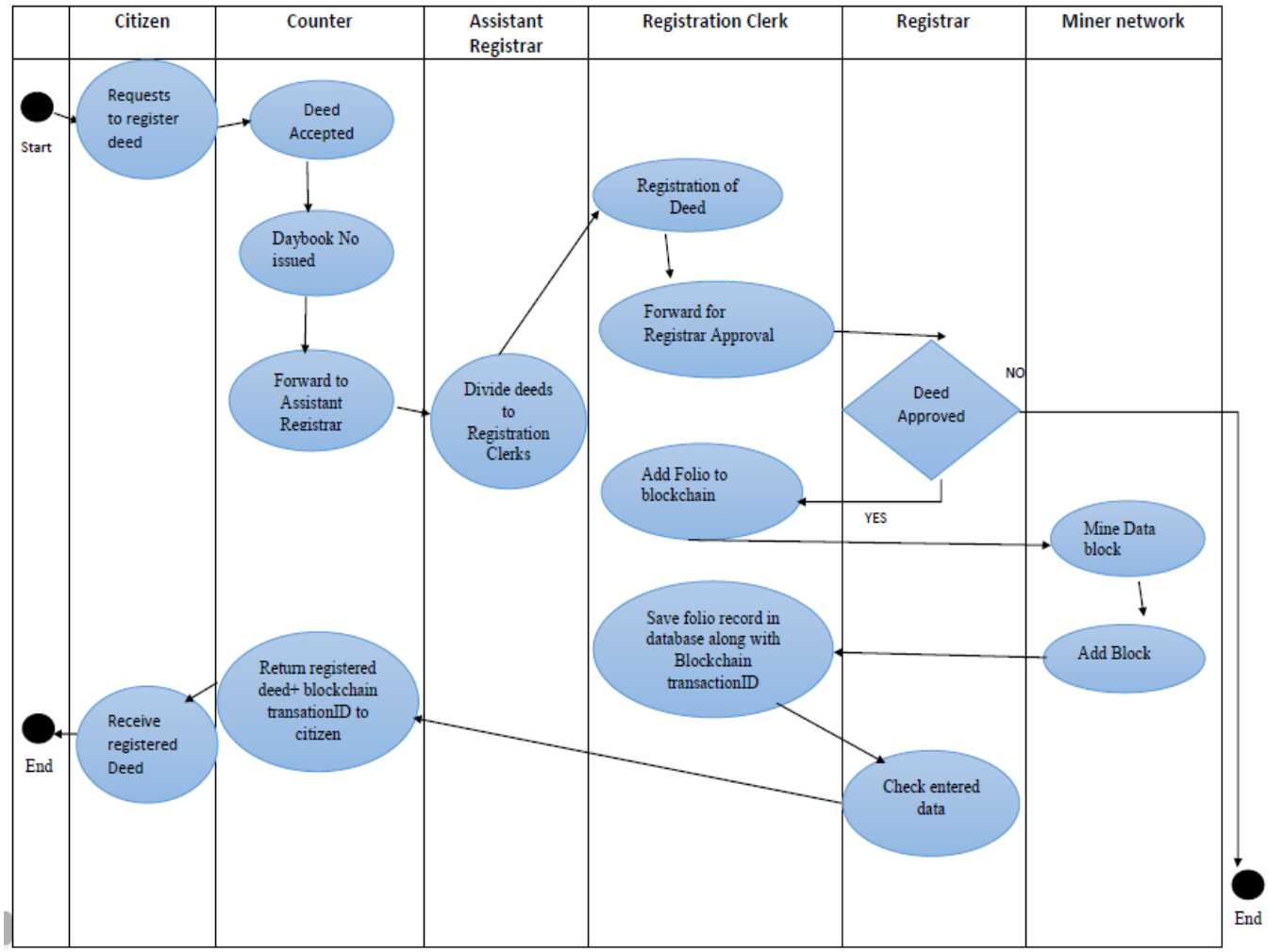


Figure 13- Activity diagram of Registration Process

3.2.2.1.2 Document Retrieval

When a citizen request a copy of a Deed or Folio stored in Land Registry Office Citizen

- Submit an application with required details to locate Deed or Folio.

Operator

- Query the database+blockchain using provided details and provide a copy

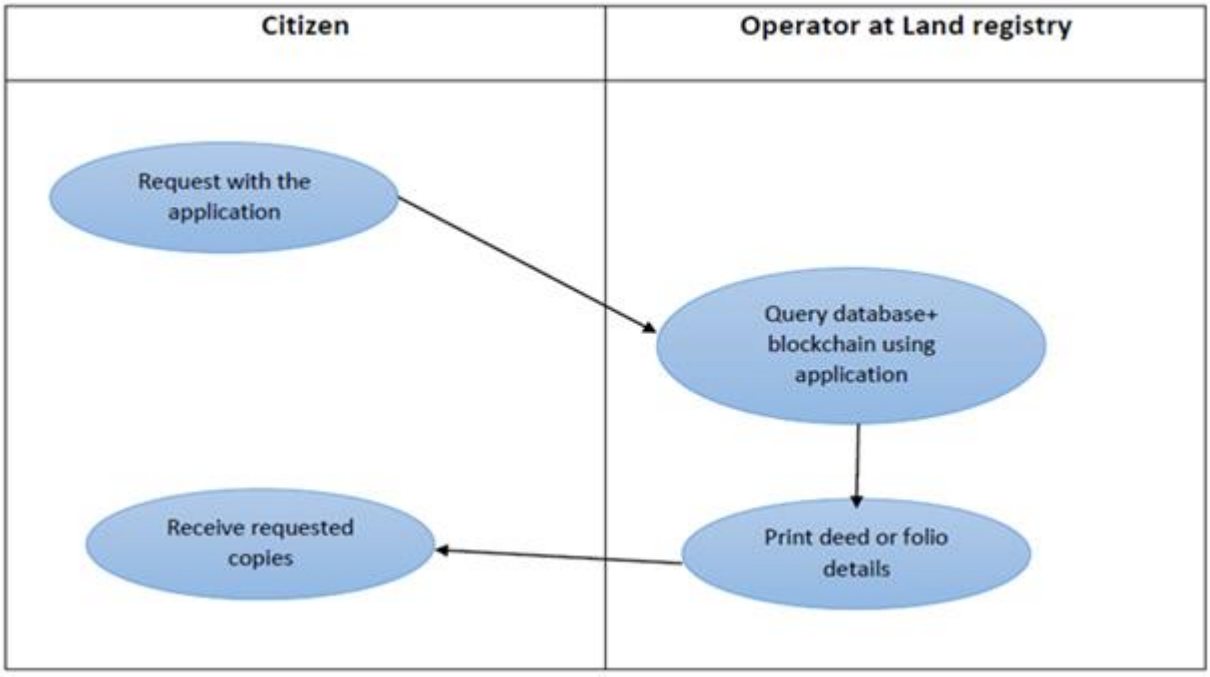


Figure 14- Activity Diagram for Document Retrieval

3.2.2.1.3 Viewing certificates stored at Land Registry Office

For verification purposes, external organizations

- Get access through a portal
- Query using blockchain transactionID
- View required folio record

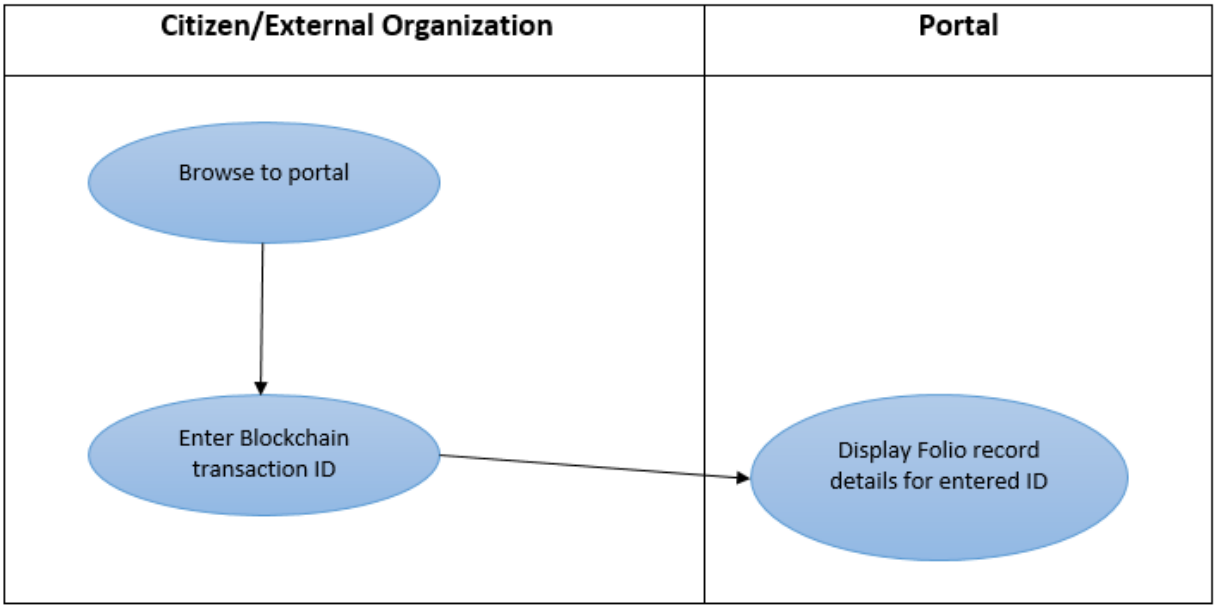


Figure 15- Activity Diagram for viewing certificate

3.2.2.2 Designed Block Structure

Figure 16- Designed Block Structure for Land Title Management

3.2.2.3 High Level Architecture

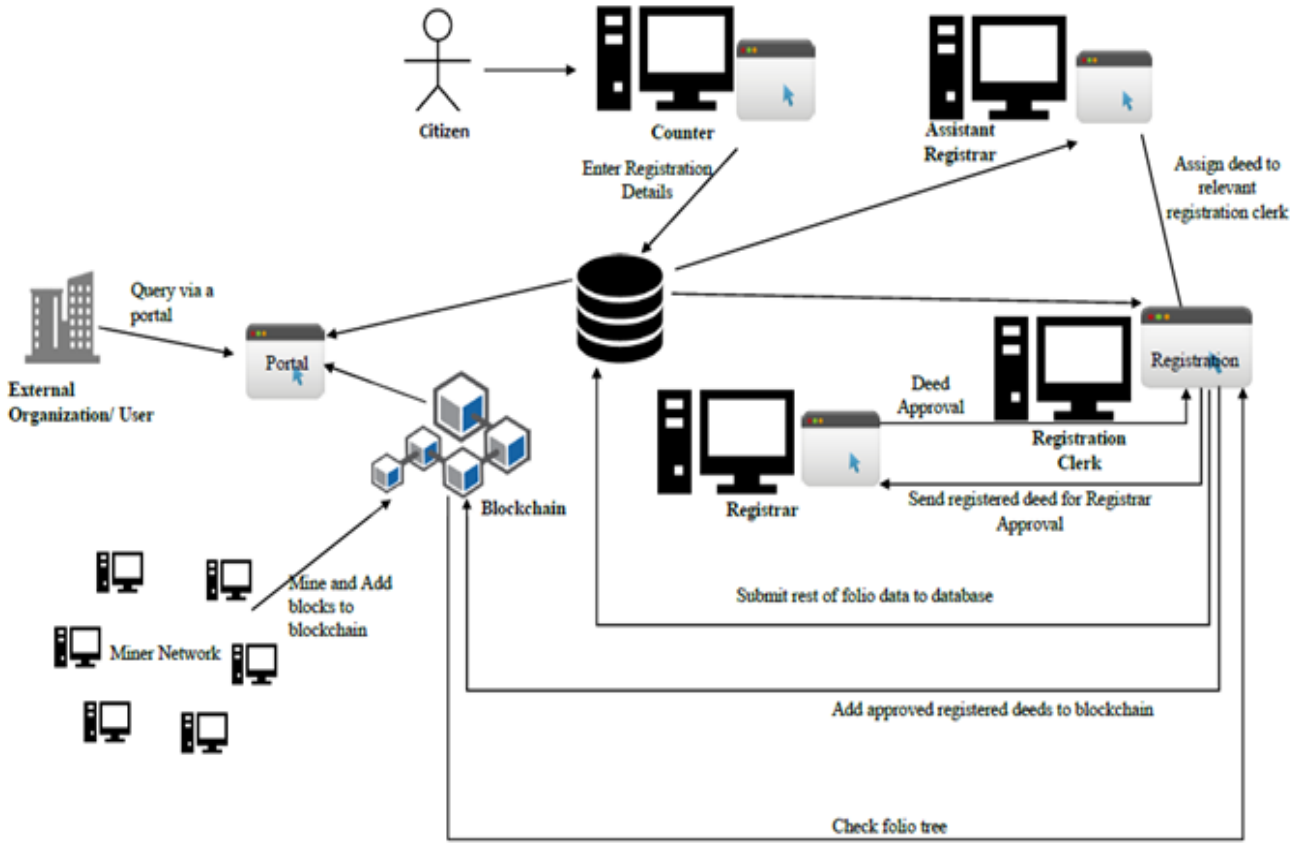


Figure 17- High Level Architecture of Land Title Management System

3.2.2.4 Design Evaluation

When evaluating the design against the identified issues, the main concern of frauds can be addressed. Since the data that verify the ownership for a particular land is in the blockchain, they cannot be deleted from the original place based on the "append only" feature on blockchain. Even if the scanned copy of deed is replaced with a forged one, since the hash value of the original certificate is in the blockchain, frauds can be detected. Digital signature of the Registration Clerk is added with blockchain token to maintain the accountability.

Data loss is also addressed because even if the database crashed and become unavailable, the blockchain transactions will be there. Since every node in Land registry has a copy of blockchain, even if 99% of nodes are down, system can be still recovered with the use of the single node which was not down.

Since blockchain is decentralized and every node has a copy of blockchain real-time accessibility for verification also can be promised because of availability is greater. Even though a portal is there, it can be queried using the blockchain transaction ID. Therefore only the people who has that ID can access. Blockchain transaction ID is not assumable because it is a complex number. So privacy of the folio records are ensured with the owner. Through the portal, real-time verification of folio records can be done by searching using the blockchain transaction ID received with the registered deed.

Merkel tree is there in the block structure. So if one token in a block is forged, that particular token can be identified by going through hash values of Merkel tree.

3.2.3 Electronic Health Records Management System

Along with the e-government initiative which was implemented around year 2003 Information and Communication Technology Agency [ICTA] has initiated an e-health program to computerize the public health records as well. Currently ICTA has implemented an open-source medical records management system. The system is designed to replace paper records while covering end to end processes of a hospital; such as lab tests, drug issuance processes, and report generations [52]. In the current context the system is implemented across nineteen clinics with standalone databases. From the above maintained nineteen locations, in some locations the system is implemented covering all main departments such as OPD and other wards while some of the systems are only limited to specific departments or clinics. Furthermore ICTA is attempting to implement the system across another two hundred locations within this year. It should be highlighted that ICTA is operating with plans to create a national patient database for the country [53]. Hence at the latter stages all those standalone systems will be integrated with each other [54].

In the existing e- health records management system; it uses a relational database to store patient details. It is a MySQL database with 90 tables and it handles all the data which are generated in day to day hospital operations [52]. Once a new patient comes to obtain medicine his/her personal details are collected through a manual form and the details are added to the "Patient" table in the database. A unique identifier is issued to each new patient. The identifier will be the PID [Patient ID] of the patient table. All the relationships in tables regarding a particular patient are defined based on the PID. Hence the PID is used to retrieve data from the database. Each patient will be issued a patient card which contains his/her personal details along with a barcode. Barcode contains the PID of that particular patient. This PID is being used by the different departments within a hospital to interact with the patient and to update the patient's' medical records.

In the existing system a relational database management system [RDBMS] is used to store all the data. Hence the identity related details are also included in a separate table called "Patient." Usually doctors and other related medical practitioners have access to the "Patient" table and given the chance to read identity related data of the patients. When analyzing the current system we observed that there is very less chance that a particular patient can obtain

medicine without keeping his/her identity as a secret. Patients have their patient card with them and should provide it to the hospital staff when it is requested. The patient's name is printed on the patient card and any person can just get to know the identity of a patient by just looking at the patient card. Furthermore patients are unaware of how those personal details are used, who have accessed his/her personal data and how often his/her details are accessed in the hospital. Sometimes this may directly discourage some patients to come to the clinics and obtain medicine. For an example a patient who is suffering from a cancer may be not interested in exposing his/her illness to any party. If he/she gets to know that those critical information is open and can be accessed by many parties without his/her consent; they may be get discouraged to come to the hospitals and obtain medicine.

When analyzing the issue, it is clear that the issue is mainly centered on the relationships of the RDBMs. This privacy concern is mainly caused by maintaining all personal data along with medication information. If there is an effective way to separate medication details, lab reports and other medical treatment information from the identity related data of patients this privacy concern of patients can be addressed to some extent.

Even if we split the data to two parts and store data separately in two databases still there will be some concerns about accessing patient information without their consent. Even though databases can restricted though access controls; but still there is a central database administrator who have all the control over the database. If the database administrator has any intention over manipulating data or if some intruder can get the administrative privileges the possibility of performing a data manipulation is very high. Hence putting your trust on a database administrator is not ideal in such situation. Hence it is important to develop a system that is not centrally controlled.

Considering the above mentioned issues, the proposed system will be focused mainly on ensuring the patient's privacy. It is true that hiding patients' identities may not be applicable in all clinical situations. For an example, in the normal clinical situations hiding patient's identities may not be suitable. But there are some clinics where hiding patients' identities is necessary. Hence the design will be focused on developing a system that would suit such situations.

3.2.3.1 Privacy in Healthcare Industry

Even from the beginning of the western medicine the privacy of patients have been considered as one of the top most priorities. However, the Hippocratic Oath is considered as the fundamental document where the patient's privacy is highlighted as a concerned area for medical practitioners. Oath is re written by Louis Lasagna in the year 1964 and it is been considered as the most commonly used Oath in the modern days. Even in that particular document there is a separate phrase regarding the patient privacy.

"I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know. Most especially must I tread with care in matters of life and death. If it is given me to save a life, all thanks. But it may also be within my power to take a life; this awesome responsibility must be faced with great humbleness and awareness of my own frailty. Above all, I must not play at God." [55]

Hence it is clear that the privacy preservation of patients is being a common concern in the medical industry for a long period of time. Even After hundreds of years; privacy is considered as one of the core ethical practices in the medical field. In the modern world apart from the ethical obligations; doctors also have some legal obligations towards patients' privacy as well. However in order to protect patient privacy it is important to clearly identify what is meant by privacy in the medical industry. As it is quoted above even Hippocratic Oath does not specifically mention what is actually meant by "Privacy." In the electronic health record management system we view privacy as the system's ability to hide the individual patients' identities while using the system. Patients should be given the opportunity to obtain medicine without giving away their personal identities. Furthermore, it can be described as the right of individuals to take decisions regarding his/her own medical information. According to electronic health record management system scenario; we cannot actually restrict the doctors accessing medical records, prescriptions since it will restrict the doctor's primary activities. However still efforts can be made to restrict accessing that personal information without prior consent of the patients.

If we analyze the medical industry in the past; it is clear that most of the medical records were in papers, files and doctors had the control over those critical data. But protecting privacy has become an even harder task with the development in data communication technologies.

Nowadays medical data is not controlled by the patient or the doctors. In the international context most of those data is managed by third party organizations as their strategic assets. Even Though in the Sri Lankan public health management system context; the data is owned mostly by the hospitals which means that there is very limited intervention by third party data brokers, health trackers, medical websites. However still there are several concerns about privacy of patient data as well. Apart from the doctors other parties such as data entry operators also engage in managing the patient data in a hospital. Hence there is a possibility that critical medical information may be exposed to outside world.

If we consider the typical scenario of a hospital; in the staff of the hospital there are two categories of people who may have interest in someone's medical records. First category is the people who actually don't know anything about your personal details. Even though they get to know about your medical status still they don't know about your personal identity. Even though if they have access to patient's medical records; if they don't know the patient's identity it will not be useful. Hence their primary focus would be getting to know your identity. Second category of staff may know the patient's identity. Since they know the patient's identity they don't have a need to look into your personal information such as name, address and job. Hence there primary focus would be obtaining the patient's PID. If they can see your PID they can just use that to query though the medical data. Hence it is important to highlight that exposing PIDs is not suitable. If the PID of a particular patient is open and can be viewed by everyone then there will be less chance to defend the privacy of patients from the second category of people. Hence our solution should focus on addressing that issue as well.

3.2.3.2 Other issues in the existing system

As it is mentioned in the earlier chapters it is clear that the main issue which exist in the electronic health data management system is the privacy of the patients. Since the design is mainly focused on developing a system that could address the privacy concerns. Along with the privacy concern there some other issues that exist within the existing system as well. Due to the availability of loosely connected standalone systems there are very high chances of data loss as well. If the data in a particular hospital is loss; the medical records cannot be replicated from other hospitals. Furthermore, accessibility from different locations is also problematic. As it is described earlier due to the availability of standalone systems the data is isolated within hospitals. Doctors only get the opportunity to view medical records which are created with in

that hospital. Even though it is not that much prominent the system also has some concerns related to data manipulation as well. All the data is handled by the hospital staff and patients may not get a chance to alter or see his/her personal medical records. Hence the medical staff and the system administrators have more control over the patient data. Furthermore, data manipulations are also possible though intruders. Hence the Blockchain based solution should also focus on addressing those issues as well.

3.2.3.3 Proposed Blockchain Based Solution

As it is described in section 3.2.3 it is clear that the privacy of the patients is being mainly challenged in the current system by maintaining identity related details along with medical records. If we consider the medical database in the existing system it contains all the patient details, diagnosis details and medication details as well. Hence in our proposed solution we attempt to separate the medical information from the identity related information of the patients.

In the process of separating those medical information and identity related information, it is important to note that it is not feasible to go for a complete blockchain based solution due to the highly volatile nature of the medical records and specifically due to the storage concerns [56]. Hence, we do not propose to store all the data in a blockchain. We attempted to decompose the schema of the "patient" table in order to develop a privacy preserving system.
As the first step of the suggested approach we attempt to separate the initial personal details of a patient from the database.

"Personal details" refers to the fields of the Patient table which are possible to use in order to identify a particular patient uniquely. [Eg: Name, NIC No, Address] And there are some fields in the "Patient" table which cannot be used to identify a particular person directly. [Eg: DOB] However the presence of such details can be used to locate a specific person in some situations. Hence these data will also be separated from medical data. However, it should be highlighted that this decomposition is done only to the data in the "Patient" table in the existing database. If we consider the data in the medical database there are lots other data of a particular patient such as diagnosis records, medication information. Those things also may be also categorized as personal data. But we do not take those data to the decomposition effort. Hence we only decompose the data in the "patient" table. Hence, we do not apply this categorization to the other relevant tables which contains diagnosis and medical information.

Our attempt will mainly focus on developing a privacy assured system only by decomposing the patient table and the data of the "Patient" table.

3.2.3.3.1 Patient Creation Process of the Suggested System

As it is explained in section 3.2.3, a data entry operator is engaged with input of personal details to the system and once a new record of the patient is created a unique PID is created by the database for that particular patient. It is important to highlight that this PID acts as the primary key for the medical database and all the relationships (regarding patients) within the database is developed based on PID value.

In our approach we will only add the PID to the Patient table in the relational database. At this point the unique identifier for the patient record [PID] will be generated from the medical database. Hence the existing "Patient" table will be altered and restricted only to store PID. However, it should be highlighted that the relations in the existing electronic health record management will not be affected. Due to the availability of the key field "PID" all the relations in the RDBMS is not compromised. Only difference would be that there will be no personal details stored in the "Patient" table. Hence anyone who has access to the "Patient" table cannot see any personal details such as Name, address, etc. There will be only a single column to store the PID key values. The relationships in the database will remain unharmed since the primary key "PID" is not removed. Due to the availability of PIDs the medical practitioners can continue the use of existing electronic health record management system as it is. However it should be highlighted that any person who have the full access to the medical database can only see a list of PIDs. They can't specifically identify a particular person since the personal details are not stored in the medical database.

In our suggested approach the blockchain will be utilized to store all the personal details of the patients. Once a data entry operator submits the details of a patient, the system will obtain a new PID from the database for the patient. As this point the system will also generate a unique symmetric key for the patient as well. The symmetric key will be a randomly generated number which contains twenty alphanumeric characters. All the personal details (such as name, address) and the PID of that particular patient will be encrypted separately using the unique symmetric key and will be stored in the blockchain as a single transaction. Hence as it is displayed in figure 20, any person who have the full access to the medical database can only

see a list encrypted values. He/she may not be able to read personal details of a patient directly by just viewing the blockchain. As it is described before exposing the PID to outside world is not acceptable. Hence in order to identify different transactions which are unique for a particular patient in blockchain we have introduced a separate key value as SID. SID is a randomly generated number which contains ten alphanumeric characters.

The next step of our suggested approach would be providing the ownership of the personal data set of a particular patient to its owner. In order to achieve that we have introduced two options. A simple mobile application and the existing barcode card approach. For the people who are capable of using mobile applications we have utilized the mobile application approach and for the people who are unable to utilize the mobile application, the barcode card method would be utilized. A mobile app or the card would only contain two parameters. The SID of a particular patient and his/her unique symmetric key. Whenever a doctor needs to view the patient's medical records in the medical database doctor needs to obtain PID of the patient as it is displayed in Figure 19. If the patient doesn't want to expose his/her identity he/she can only give the PID. Once the PID is provided doctor can have a look on medical records but still have no idea about the patient's identity. If the doctor needs to know the identity related details then the doctor should request the relevant symmetric key from the patient. Otherwise there will be no other way to decrypt and view the personal details of the patient. Hence in the proposed system the identity of the patient is only revealed if and only if the patient gives away his symmetric key.

3.2.3.3.2 Patient Creation

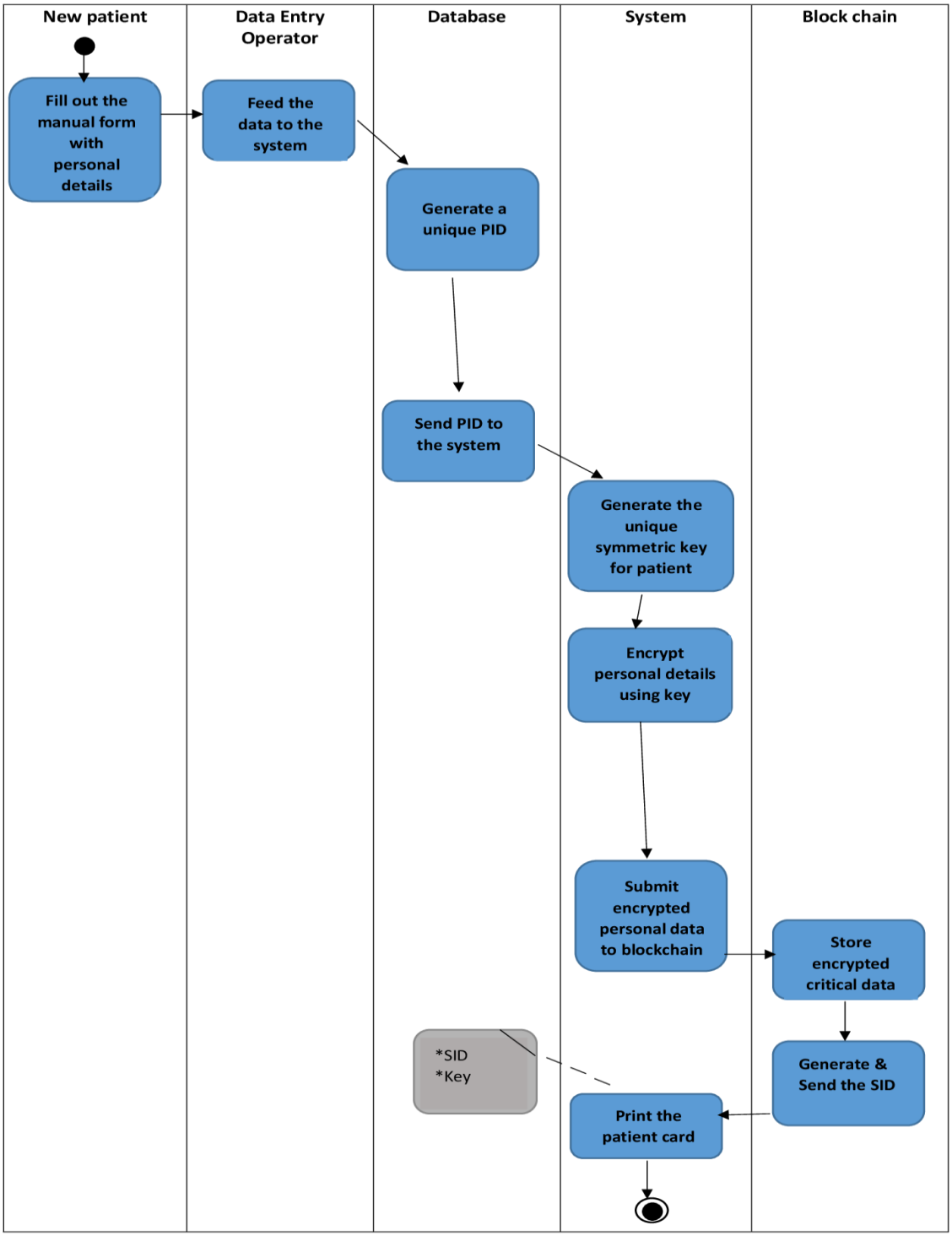


Figure 18- Activity Diagram for Patient creation

Since all the critical data in blockchain is encrypted the patient's details will not be disclosed to any party without the consent of the patient. Even if a doctor wants to view the personal details of a patient; the patient will have to provide his key to the doctor. Since the personal information disclosure will be done only with the consent of the patient. Even to access the medical records of a particular patient a doctor will have to obtain the PID of that patient through the blockchain. As same as the above process it will be only done with the consent of the patient.

3.2.3.3.3 Patient Data Retrieval Process

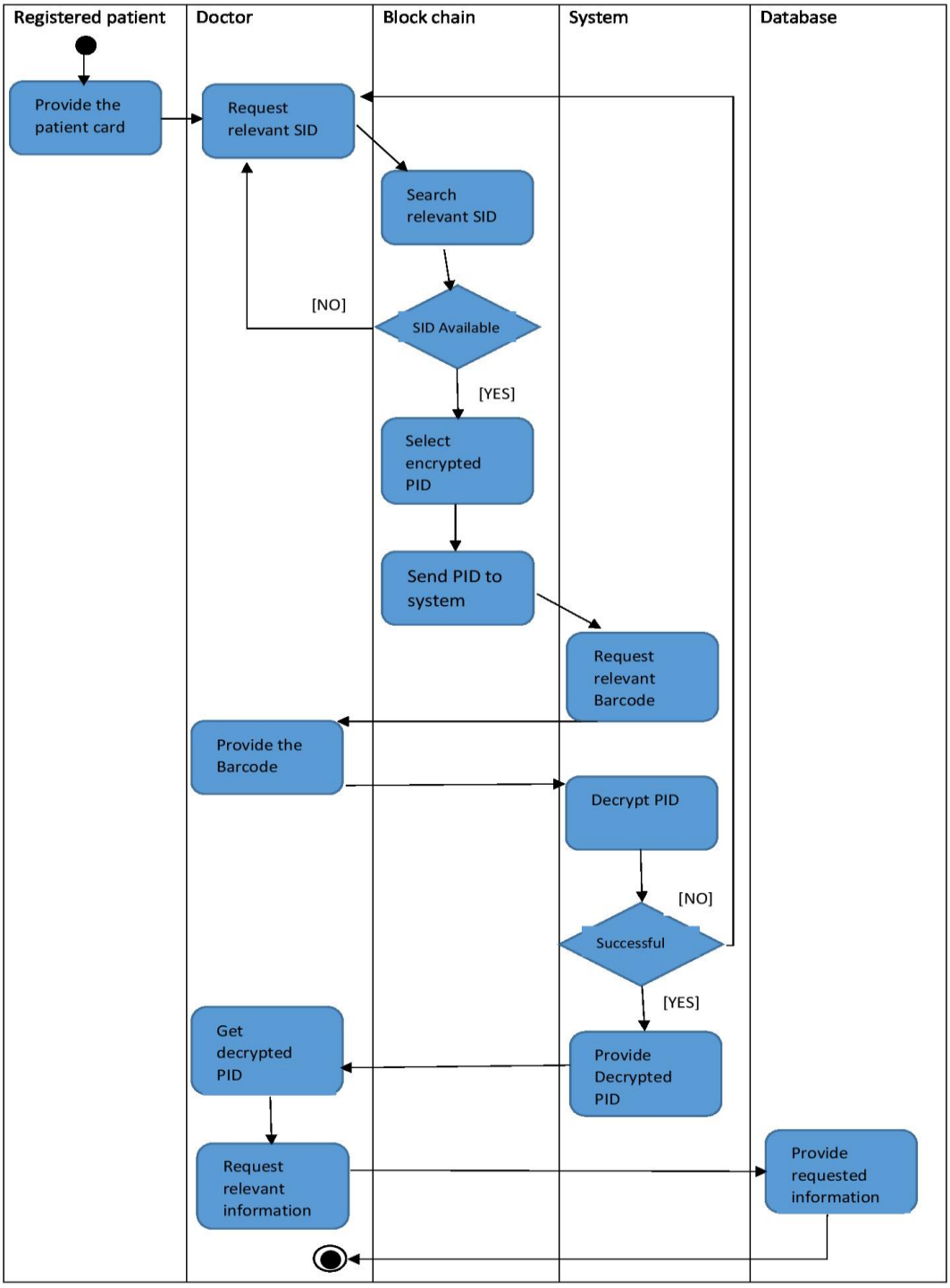


Figure 19- Activity Diagram for Patient Data Retrieval

3.2.3.4 Designed block structure for e-Health Blockchain

Block No: 102

Block hash: 00023424f6587d0097r8765t342g143b6dfk559

Nonce Value: 43760076

Previous Block Hash:

Timestamp: 11.9.2017:23.57

Mined by: Colombo South

Merkel root: G4565H22345A54666655FFAA578899TD

No of patient records:03

SID	First Name	Last Name	Address	DOB	NIC	PID	Time
0043	VUv6a68e	3ysdF0dEk	zHGDPjOV1	0SwqLCtlk	geVXT0a	nj3ga+Yt/Y=	9.9.2017:20.33
0046	pJBv5W5j	a/0ryqp90/	+gmU0Mw	ittVrfAEzfu	kBXfdirN	LkK2owe	9.9.2017:22.41
0043	cRpeeGmv	PtauwPC5k	tn4e1UQdgbsjk	m72Sg8fqp/	JbKyLzAUn	nj3ga+Yt/Y=	11.9.2017:23.33

Figure 20- Sample Block Structure for Health Data-1

Block No: 103

Block hash: 0004f6Yfa43ffd0097r8765t342g1gg5a7t34dd

Nonce Value: 54329472

Previous Block Hash: 00023424f6587d0097r8765t342g143b6dfk559

Timestamp: 12.9.2017:14.33

Mined by: Colombo North

Merkel root: 3FF5AF22345A54666655F451SRT3CFF7

No of patient records: 05

SID	First Name	Last Name	Address	DOB	NIC	PID	Time
0048	nK6/0SwqLCkbf	hDsnffbdT	pGi1Iwwbfa7K0o	Orqo7N1	0dRqCGY	Jh7v0kWPq38	12.9.2017:08.33
0043	PePB0qMON	mNbVy2rvCE	+71XPbgUTjw	oj4x8Ur	kw5cmoD	TJcnRrA=	12.9.2017:08.41
0049	4x8Urou	Xeg9/qMi	wIPGFD0	ouckQEtS	TtE8qliglq	KAVQA==oj	12.9.2017:10.23
0050	ckQEtSKAVQA==	3ab/3CD3	lFYve0xtB	Orqo7N1	wwSfiR	e2xU9BC	12.9.2017:10.37
0052	v+qSN0A	Aw84C0y	apS3y1q1	uqy4i+faV	BbUrB0b1	VxH4Ague	12.9.2017:11.33

Figure 21- Sample Block Structure for Health Data-2

Figure 20 and Figure 21 demonstrate the two consecutive blocks of the proposed blockchain. As it is displayed in the figures, all the personal details of patients are encrypted and the relevant key for decryption is only held by the patient. As it is showed in Figure 20 the shown values are instances of encrypted values. Records with same SID displays several records which belongs to the same patient. When there is a requirement to edit personal details of a particular patient it will be added as another transaction.

3.2.3.5 High Level Architecture of the System

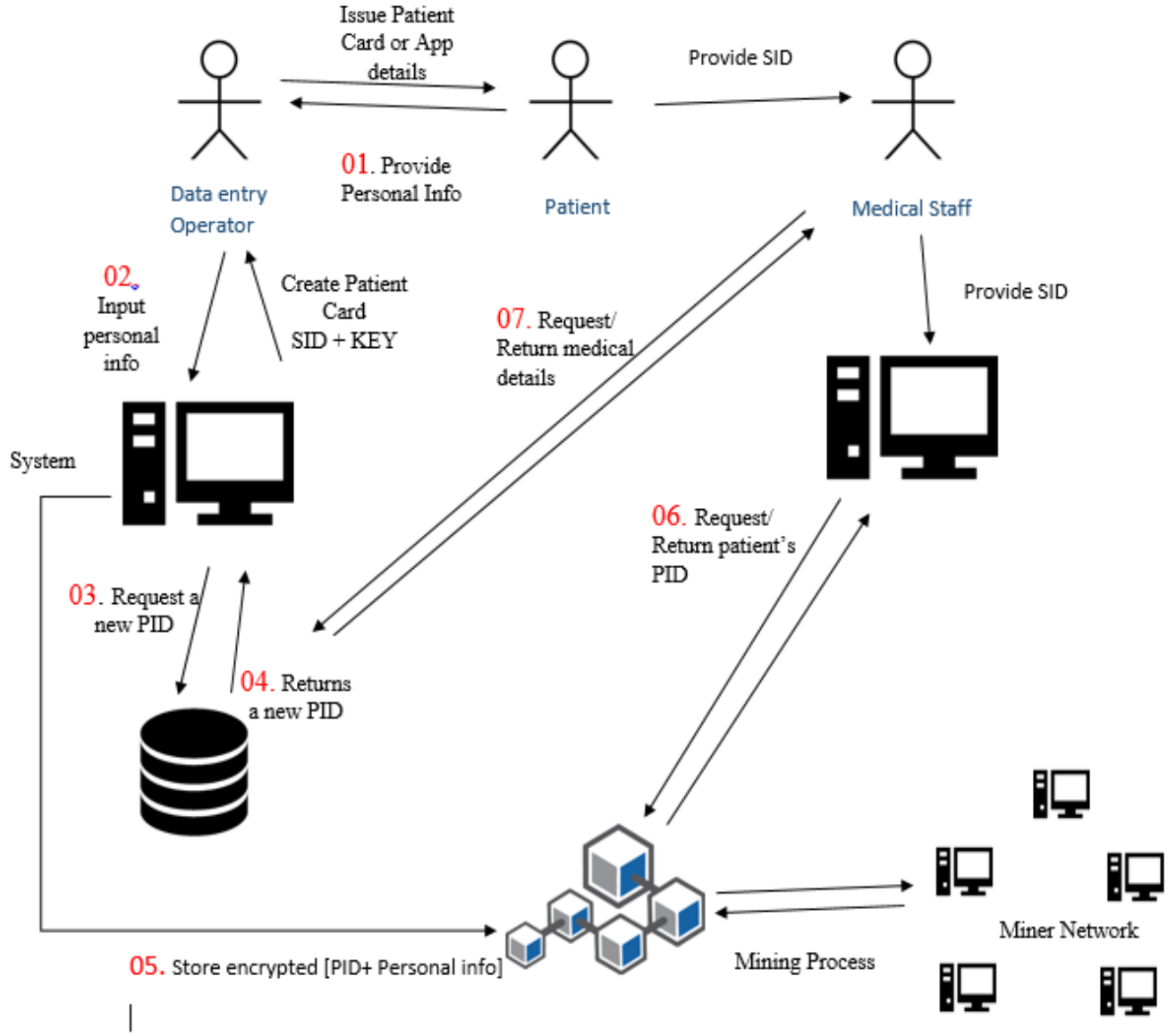


Figure 22- High Level Architecture of Health Data Management System

3.2.3.6 Evaluation of the blockchain design

Addressing the data privacy issue

In the proposed Blockchain based solution the patient will have the ownership of his/her personal details. These capabilities are achieved by using symmetric keys along with blockchain capabilities. Every patient will be issued a symmetric key. That symmetric key will be held by the relevant patient in a mobile app or in a barcode card. This key will be only kept by the patient and no one will have the access to that particular key. This key will be eventually used by the data administrators in order to encrypt the identity critical data set. Those identity critical data set will be encrypted and stored in the blockchain. Each and every time when a medical practitioner wants to access those personal details or PID he/she will have to obtain the consent from the relevant patient. If the patient agrees to give away his/her PID and personal details he/she can provide the symmetric key. Patient will have to give the permission to access the PID by giving away the barcode card or by providing the permission through the mobile app. If the patient refuse to provide his/her key then no one can obtain the patient's PID or the personal information. Since the total ownership of those identity critical data set will be transformed to the patient.

As it is described earlier, there are two categories of people who may have interest in someone's medical records. First category is the people who actually don't know anything about your personal details. Even though they get to know about your medical status still they don't know about who you are. Even though if they have access to patient's medical records; if they don't know our name and other personal details it will not be useful for them. Hence they may be concerned about your name, address and job. Second category refers to the people who have some knowledge about your personal information. They may know exactly who you are and they don't need to look into your name, address and job. Hence they are only interested in getting to know your PID so that it could be used to look into medical information. If we consider the first category of people; they are directly interested in getting to know your personal information such as your name, personal address, NIC. In order to restrict first category of people, hiding the identity related details would be enough. However it would not be enough to restrict second category. Second category is the people who know the personal details of a particular patient. Since they know the patient's personal details they may not be

interested in looking into those details. They [people of 2nd category] are only interested in getting to know the patient's PID so that it can be utilized to extract to obtain data from medical database. Hence the PID should also be restricted or hidden. Hence it is not feasible to use the PID openly. Hence we can't utilize that as the ID in a barcode card or as the ID in the mobile app. Hence we have introduced another key value as SID; which will be utilized as the app ID or the barcode ID. This SID will be used as the key value for mobile apps and barcode cards. Furthermore All the PIDs of patients will be encrypted and stored in the blockchain. Hence, we have restricted both two categories of people from accessing the medical information.

Addressing the data manipulation possibilities

We have directly utilized the "append only" nature of the Blockchains to restrict the data manipulation possibilities. As it is explained in the design chapter the blockchain contains all the personal data of a particular patient. Furthermore, the data which can be used to identify a person directly (eg: Name, Address, PID) would be stored after encrypting. Hence even a person who has full access to the blockchain can see only the encrypted values. They can't read the PIDs, names directly by viewing the blockchain. Hence any intruder cannot directly identify the record they must manipulate by just looking at the blockchain. Without properly identifying the specific patient; manipulating a record would be pointless.

The next option for an intruder would be manipulating a random record. If an intruder randomly selects a record and update it, still the updated record will not replace the previous record. Due to the "append only" nature of Blockchains it will create another record in separately along with the same SID. Hence anyone who has proper access to the blockchain can monitor or view the list of changes which are done to a particular patient record and clearly identify who has done the change and what change is done.

The next option for an intruder would be accessing and manipulating records in the database. If an intruder can obtain the relevant access privileges to the system he/she can manipulate the records in database. However, it should be highlighted that with the decomposition strategy which we used in our design; the intruder doesn't have any proper way to specifically identify a particular patient. In the database it will contain a list of PIDs and its relationships. The relationship between the PIDs and patient's details are recorded in the blockchain. Furthermore, all those PIDs and patient information is also encrypted using the

symmetric key. And the key is only kept by the patient. Even though an intruder has the full access to the database he cannot isolate a specific person and edit his/her personal records. Only thing intruder can achieve is that the manipulation of some records randomly without knowing the real patient.

The worst-case scenario would be a particular patient having full access to both the blockchain and the database. Even in this scenario identification or the isolation of a particular patient is not possible without a patient providing his/her symmetric key. Hence the manipulation of records has been effectively restricted in the proposed system.

Addressing the data loss possibilities

In order to address the data loss possibilities of the existing system we have utilized the decentralized nature of the blockchain concept. In a blockchain based solution there is no need to maintain separate backups. All the data in such blockchain system is replicated among all the nodes. Hence the encrypted PIDs and critical personal information is replicated among several nodes. Each and every node in the system will maintain the exact same copy of the dataset at each separate location. Even in a situation where several nodes have lost their data the information can be quickly recovered from a single active node. Since in case of a failure a particular node can obtain all those details with in few seconds. Hence the data loss possibilities can be minimized in a blockchain based solution.

However, it should be noted that the blockchain don't have any control over the data which are stored in the database. If the medical database comes across some kind of a failure then they will have to utilize the existing recovery options of the database. Usually all those critical data centers maintain separate backup plans and Business continuity plans to ensure the continuous availability of the data. Data should be recovered utilizing those options. However even in such situation critical personal information will remain in the blockchain without any failures.

Addressing the Data accessibility issues

In order to address the accessibility issues, we have utilized the decentralized nature of the Blockchains. All the nodes which are connected to a particular blockchain will maintain a

complete data set of the particular system. Since once a particular point of the network request to access the data; the access can be easily provided by initiating a blockchain node at that point. After the relevant permissions are granted; that point of the network will have full access to the blockchain and will continue to listen to the transactions in the network. Hence all the encrypted PIDs and critical personal information can be accessed from anywhere if that particular node has relevant access permissions.

3.3 Generic Guideline/ Framework for public data management

In global context there are many different existing Blockchains like Bitcoin and Ethereum which have been developed over the years and now being used as sustainable platforms to deploy various projects and experimental systems which associate blockchain concept. However, when selecting a specific blockchain platform to build a newer Blockchain project or to implement it from the ground level, for public sector data management, there are different aspects that need to be considered such as the nature of the blockchain and extent of usage. Based on existing literature, we designed a generic guideline that can be used to select a suitable blockchain approach for public sector.

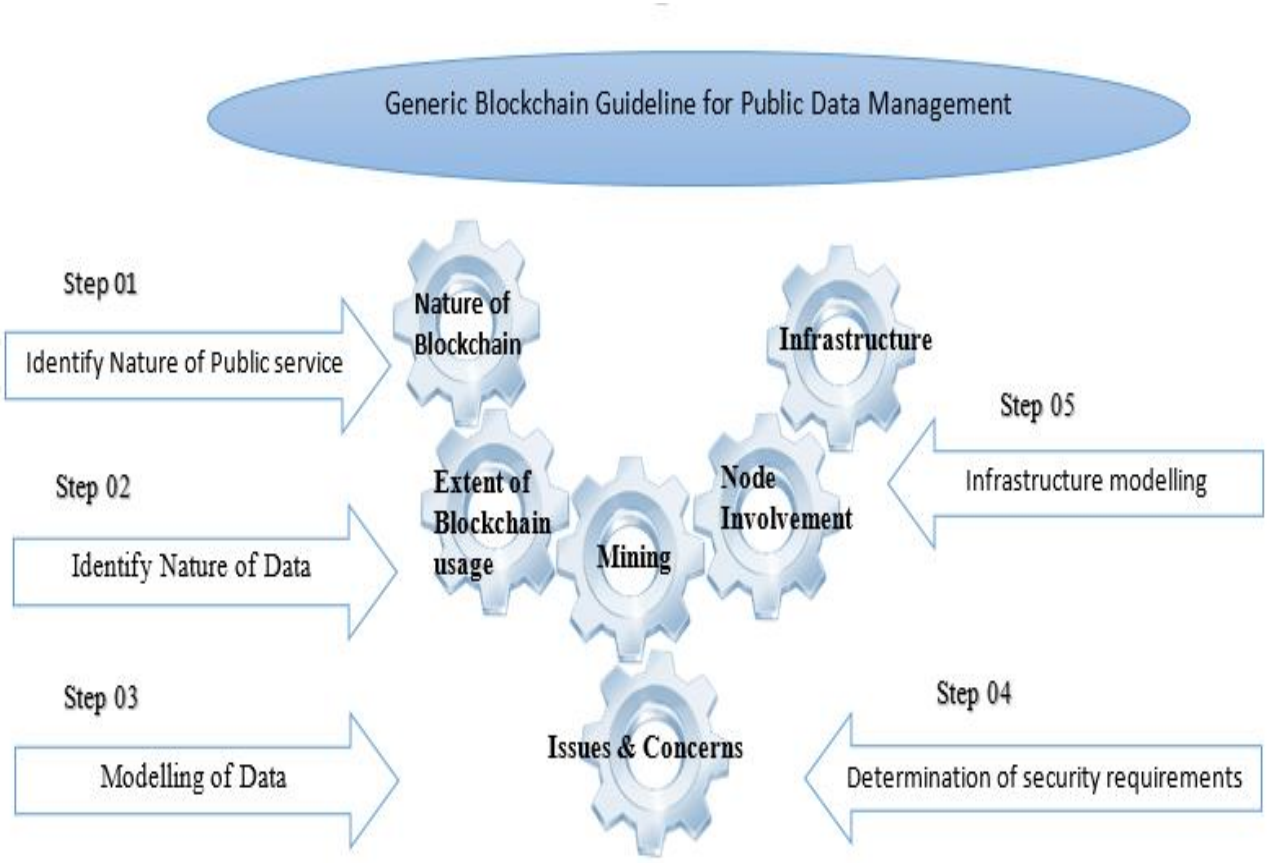


Figure 23- Generic Guideline to Build a Blockchain

The Generic Framework/ Guideline we designed for Public Data Management of Sri Lanka comprises of six components and five main steps that should be considered when implementing a blockchain solution for a public data management system.

The six components are namely,

- Nature of Blockchain
- Extent of Blockchain usage
- Mining
- Node involvement
- Infrastructure
- Issues and Concerns

3.3.1 Nature of Blockchain

There are four main categories of Blockchain as,

- Public Blockchains
- Private Blockchains
- Public Permissioned Blockchains
- Private Permissioned Blockchain

In a **Public** Blockchain, any node can read and write the data stored on the Blockchain as it is accessible to everyone in the world. Any person can become a member of the Blockchain network to store, send and receive data after downloading the required software on his device. A Public Blockchain is completely decentralized where the permissions to read and write data onto the Blockchain are shared equally by all the connected users, who come to a consensus before any data is stored on the database. A Public Blockchain is based on a completely trustless system where no user is given special privileges on any decision [57].

In a **Private** Blockchain, the permissions to write data onto the Blockchain are controlled by one organization which is highly trusted by the other users. This organization may/may not allow users to have access to read the data, as public readability might not be necessary in most cases. In some situations, the organization might want the public to audit the data. Limited/restricted read permissions also provide a greater level of privacy to the users, a feature not available in Public Blockchains. The organization in control has the power to change the rules of a Private Blockchain and may also decline transactions based on their established rules and regulations. In a Private Blockchain, the transactions are quicker as they can be verified through consensus by a small number of devices. There number of people verifying the transaction is fewer than in a Public Blockchain [58].

A **Permissioned** Blockchain is a hybrid of a public blockchain and a private blockchain. It often referred as a Consortium Blockchain, where instead of allowing any person to participate in the verification of the transaction process, a few selected nodes are used for mining and verification [57].

The blockchain solution which is ideal for data management in government organization as we suggest is a private permissioned blockchain based on several reasons. One of the main reasons behind the suggestion is the extent of control, of blockchain that should be given to a particular organization/ government institute. Since the information stored on the Blockchain is sensitive and mostly personal information with regards to citizen of a country when allowing the permission to access the Blockchain, a form of access control is a necessity. And when it comes to the Mining functionality it needs to be under the authorization of the particular group of mining representatives of each public service delivery organization which will make a network of private miners making the Blockchain a private Blockchain. Since the designs does not involve a compensatory mining mechanism as well as the requirements of customized block structures with respect to each and every public service delivery system this is a necessity. Therefore, it limits the opportunity to go for a tradable token concept like in BitLand [41] or simply using an existing Blockchain like Bitcoins to get the mining process done. This is also backed up by the time it takes to get mined in a blockchain like such.

3.3.2 Extent of Blockchain usage

Blockchain can be used for Data Management in several methods as,

- As a single Database option
- As an Access Control mechanism to limit access to a separate Database
- As a privacy preservation option
- As a verification repository

If the Blockchain is used **as a single database solution**, all data should be stored in the blockchain itself. There the mining will be costly because of the increase of block size and the time it takes to conduct the mining function, since the mining effort required will increase with the block size or in other words the size of the data in a particular block [58].

If the blockchain is used as an **Access Control Mechanism**, the critical data that needed to be protected against viewing/modifying by every user in system can be separated from a

traditional database and that specific data can be stored in the blockchain with a pointer to the original database, creating limited access to the original database.

If the blockchain is used as a **privacy preservation option**, the sensitive data that need non-disclosure can be removed from the original database and store them in the blockchain.

If there are documents or files that needs the **verification** for their originality, the hash values of the documents or files can be stored in the blockchain while storing the documents in the original database. If scanned images of certificates or documents are also included in the public data, rather than storing the particular image + rest of data as a record in blockchain, it is more efficient to store the image and non-critical data in a separate database and storing the hash value of image with other critical data in blockchain. The reason is that as mentioned in the above section, the increase of block size result in the increase of mining effort [59]. If the cost that needs to be incurred because of the requirement of high mining effort is bearable, images can be stored along with rest of data in blockchain.

3.3.3 Mining & Consensus

From the mining types stated in the literature review section 2.2.2, the ideal mining for the public data management is the customized proof of work to mine digital asset data. That is because the content of a block is depend on the particular data management process. Therefore the mining should be customized according to a particular public service delivery system process and based on the information that a particular service need to include in a block and its block structure.

3.3.4 Node involvement

Any computing device that is connected to the blockchain network is called a node. For a Blockchain network, there are several possible types of nodes as,

- Mining Nodes
- Nodes able to Query only
- Nodes with data adding functionality

For Data Management of Public Service organizations, Nodes with data adding functionality is offered to the data entry points at a particular Public Data Management

Institute. The external entities that need to query the blockchain can be offered with the Only Query functionality and the respective records can be searched according to the values that will be assigned as transaction ID in each design with respect to different public service management systems. The mining nodes can be offered to the pool of permissioned miners representing different branches of same government institution such as Divisional Secretariat offices and Hospitals because of the reasons mentioned in the sections 2.2.2 and 2.2.3 explaining the mining functionality and the nature of the blockchain associating with the cost, infrastructure and the time required to complete the functionality.

3.3.5 Infrastructure

In Order to deploy a Blockchain network different types of infrastructure needed. The mining nodes are needed to be consist of hardware with high capacity CPU and Graphic cards. Special mining software are needed to be developed with the mining protocols to be in the verification. Client nodes can run on standard Desktop specifications. If the volume of data to be stored in the blockchain is huge, high capacity storage devices are needed for every node which holds a copy of blockchain.

3.3.6 Concerns and Issues

There are concerns and issues specific to the type of blockchain application. Even though the data inside blockchain are secure, physical access to the devices holding the application should be limited only to the authorized parties simply because nature of data that is being used in public service like the personal and private data of a specific individual or a party. And simply because we need to be aware of the secureness of the data entry stage because it determines whether the information feed into the Blockchain database is accurate or not and that has a huge effect on the reliability of the information and the verification capability provided by the Blockchain. This concern leads to why we need a permissioned Blockchain for the Public service delivery systems, because of the fact that we need a point of data entry or access with an individual who will be held responsible for the correct data entry at the most initial stage so that the benefits of the Blockchain characteristics will be able to incorporate into the process thereafter. After selecting a blockchain based on the generic guideline it can be implemented and customized for a particular Data Management process. For different data management applications separate Blockchains can be used or they can be stored in a single blockchain under different streams [60].

The five key steps to be followed are namely,

Step 01: Identify Nature of Public service

Step 02: Identify Nature of Data

Step 03: Modelling of Data

Step 04: Determination of additional security requirements

Step 05: Infrastructure modelling

Step 01: Identify Nature of Public Service

As the very first step of the process, the nature of public service that is going to adopt blockchain for data management should be considered. Different public services have various concerns on decentralization of data, privacy of data, data loss and possibility of frauds and manipulation in different magnitudes. And also in each and every public service delivery system the data that should be stored in a Blockchain will vary depending on the data size, criticality, and sensitivity of data and how frequently this data is being accessed or used. Therefore when designing a particular Blockchain based design for a specific process a thorough analysis need to be conducted to identify what aspects need to enhanced and what aspects should be compromised. Systems like Land Title Management are concerned much on the possibility of fraud and manipulation than the privacy preservation. Systems like Electronic Health Record Management System value the privacy preservation than the possibility of fraud and manipulation of data. Furthermore as the users of such public services, people may have different concerns as well. For instance the users of Land Title Management system may interested in using the system as a way proving the land ownerships. Hence they may want such data publicly available and to view by everyone. On the other hand the users of an Electronic Health Record Management System would want their data hidden from other parties. Therefore, the specific nature of the Public Service should be clearly identified to select the characteristics of blockchain that need to address the domain specific challenges. The components 'Nature of Blockchain' and 'Extent of Blockchain usage' depends on the nature of public service. Therefore it's important to correctly identify in what way the Blockchain should be incorporated into the design in this phase, which simply addresses the requirement of a particular system.

Step 02: Identify Nature of Data

After identifying the nature of Public Service, identifying the data that belongs to the particular Public Service should be done. For the considering public service different categories

of data may be there based on their importance for the public service delivery. There could be a data segment, which can be considered as critical. If that data is exposed to manipulation, the integrity of the service may fall into question or if that data segment is lost, the operation of service gets interrupted. Furthermore, there may be some data that are sensitive or privacy critical where if they are exposed it could cause serious damage on the owners of such data. Frequency of refreshing of data and volume of data that gets added in a specific time period also should be identified as the nature of data. The component 'Extent of Blockchain usage' can be decided after identifying the nature of data. The specific nature of the data will decide the characteristics of blockchain that need to be utilized to support data. A system like Land Title Management holds data that defines the ownership details for a particular land. Therefore such data record can be inserted into the blockchain as a token or an asset. For data that gets update in very short intervals of time are not suitable for a blockchain due to the mining difficulty. If the volume of data is huge, it takes a huge mining power and such data also not ideal for a blockchain.

Step 03: Modelling of Data

After identifying the nature of data, the data needed to be modelled to be entered in to the blockchain. Most of the services currently have their own automated systems and operate with their own databases. This phase is focused on mapping the existing systems data structure with the new required structure. If there is a Database System already available for the particular Public Service considered, completely replicating data into a blockchain may be not needed. The data should be decomposed in such situation based on the identified nature of data. The critical data should be entered into the blockchain while the rest of data can reside in the tables in the Database System. For example, if there are scanned images of documents are in the existing system, rather than moving them to a blockchain, hash values of the documents can be entered into the blockchain for the mining convenience. As explained in the 'Extent of blockchain usage' blockchain is used as a verification repository for such system. Frequently updating data are better to be keep in the database rather than adding to blockchain, if they are not critical for the system. To establish the link between data records in blockchain and the Database System, a common key should be used. The link between the blockchain and the database should be defined according to the scenario of the public service. Based on the data that go into the blockchain, the block structure should be designed. Block header will be almost common for all systems. It should contain the previous block hash, Nonce value, Block height, Block size, Version, Number of records and Merkle root included as mentioned in section 2.2.2.

The maximum size of a record that should be entered into blockchain and the block size should decide the number of records that could be inside of a single block. Block size can be determined based on the available mining capability.

Step 04: Determination of additional security requirements

Issues and Concerns component that is specific for the considering public service decide the security requirements. Usually when data is transformed to a blockchain; all the data is publicly accessible and viewed by any node in the blockchain. However depending on the requirements or nature of the public service exposing all the data without any control would be problematic. If the data entered into the blockchain need to be hidden, for such situations options such as symmetric key encryption can be utilized. Even for the Blockchains different access levels can be provided based on the requirement.

Step 05: Infrastructure modelling

Based on the nature of Blockchain, the Infrastructure modelling should be done. For public data management, the ideal blockchain would be a Private permissive blockchain. For such blockchain, node involvement should be decided based on the nature of involved users. As explained under the Node involvement component different nodes are needed for a blockchain with different access levels. Number of different nodes needed for a particular branch of an Institute should be decided by the volume of data added per day and the number of system users. For mining, a pool of miners representing different branches of same Institute can be taken. Since almost all government public service processes are confirmed after the authorization of a responsible government worker who is assigned for the task, mining should schedule to be triggered after the authorization of such person. From examples considered, Land title blocks are mined when the number of Registrar Approved records fulfills the number of records that goes in one block. If there is a database functioning along with the blockchain, keeping regular backups of database is need to be done to ensure the completeness of data. Since every government institute has branches representing different geographic locations, replications of databases also can be kept at other branches. However, replicating the full database in several number of locations would be very costly. Hence the designers should identify the optimal number of replications that they need to maintain based on the industry standards and based on the nature of blockchain. In case of an error, the backups or replications should be used to recover the data segment that is stored in the database.

Chapter 4 - Implementation

For the evaluation of Blockchain designs two prototypes were used. Multichain [47] prototype for eHealth Record Management system and Hyperledger Composer platform [48] for Land Title Management System.

4.1 Multichain prototype for eHealth Record Management system

After analyzing the available solutions we have used Multichain platform [47] to come up with a solution prototype for the electronic health data management system. Multichain is a platform which can be used create and deploy private Blockchains. Even Though it is a private blockchain you can grant the relevant permissions to relevant users in order to grant access to the system.

Unlikely to the available other solutions "Multichain" allow us to operate with several number of Blockchains at any given time. Since we can use a single server in order to manage number of Blockchains with different configurations as well. Since it can provide better flexibility in managing different types of data.

In the following section we describe the process we adopted to configure the blockchain in order to use in three designs. Steps described below are related to the electronic health record management scenario and can be used similarly to other two systems as well.
As it is mentioned in the above paragraphs Multichain platform allows us to maintain several Blockchains in a single platform. This process is basically achieved by using "streams" [60] in the Multichain blockchain platform. Since our electronic health record management system is designed to handle a single type of data in blockchain; we will be using only one stream in our prototype solution. We have created a stream named "Patient Data" within the Multichain named "Patients." And utilized that stream as the place where we store privacy critical data of patients.

```
methv@methv-HP-1000-Notebook-PC:~$ multichain-util create Patients

MultiChain 1.0 Utilities (protocol 10008)

Blockchain parameter set was successfully generated.
You can edit it in /home/methv/.multichain/Patients/params.dat before running mu
ltichaind for the first time.

To generate blockchain please run "multichaind Patients -daemon".
methv@methv-HP-1000-Notebook-PC:~$ multichaind Patients -daemon

MultiChain 1.0 Daemon (protocol 10008)

MultiChain server starting
Looking for genesis block...
Genesis block found

Other nodes can connect to this node using:
multichaind Patients@<server-ip-address>:8347

Node started
```

Figure 24- Node start in Multichain Implementation

```
methv@methv-HP-1000-Notebook-PC:~$ multichain-cli Patients

MultiChain 1.0 RPC client


Interactive mode

Patients: create stream Patient_Data  false




{"method":"create","params":["stream","Patient_Data",false],"id":1,"chain_name":
"Patients"}

efc516a38b43e2bd0d4989264f5d0790d01d1818c4580f3500d7dff0234c70c3
```

Figure 25- Stream Creation in Multichain Implementation

Every user who have authorized to access this chain should subscribe to a particular stream in if it intends to read data from that particular stream.

```
Patients: subscribe Patient_Data
{"method":"subscribe","params":["Patient_Data"],"id":1,"chain_name":"Patients"}
```

Figure 26- Subscription in Multichain Implementation

After subscribing to a particular stream using the relevant CLI (Command Line Interface) command the subscribers can initiate transactions if they are permitted to do so. Even the transactions can be initiated using simple CLI commands. Additionally according to the permissions which a particular node possess, it can perform functionalities such as connecting to other nodes, creating streams, mining etc. Furthermore the Multichain CLI provides a variety of commands to view transactions within the blockchain using various types of key values such as txid (Transaction ID), Block hash and block height.

Furthermore in order to provide a web based interface to the system users we have used the "Multichain-web-demo" GUI. According to the system design we have also added several interfaces to provide the necessary functionalities to the users.

4.1.1 Issues in building the prototype using Multichain

One of the major concerns which we came across with Multichain CLI is that it only allows to enter transaction data as hexadecimal values. Since if it is needed to enter data in raw formats; using CLI is not recommended. Following screen shows an attempt to enter transaction data as a string.

[Stream: Patient_Data; Key:First_Name; Value: Mr.Daya]

```
Patients: publish Patient_Data First_Name Mr.Daya
{"method":"publish","params":["Patient_Data","First_Name","Mr.Daya"],"id":1,"cha
in_name":"Patients"}

error code: -8
error message:
Item data should be hexadecimal string
```

Figure 27- Multichain error in raw data insertion

As it is shown above Multichain CLI do not provide any flexibility in adding or retrieving data in raw formats. On the other hand it is not operationally feasible for the system end users to work with the CLI directly. Since we had to develop a usable front end which can be made available as the working space for the end users. In order to address that issue we have used the "Multichain web demo" web front end for data insertion and retrieval processes. "Multichain web demo" is a PHP based web front end which can be used to insert or retrieve

data from Multichain Blockchains. Although it has very limited functionalities it can be used as a workable front end for the users. But as it is mentioned in the design phase; the three systems are designed to handle data in different ways. Since according to the requirements of the three systems we have developed some additional interfaces for the system users that could enable them to use blockchain in an effective manner.

4.2 Hyperledger Composer platform for Land Title Management System

Hyperledger Composer [48] is a web based blockchain deploy application. For the development of Land Title Management system, composer was installed in a Virtual Machine. One folio record was entered as one Asset in Composer. Prerequisites needed:

- Operating Systems: Ubuntu Linux 14.04 / 16.04 LTS (both 64-bit), or Mac OS 10.12
- Docker Engine 17.03 or greater
- Docker Compose 1.8 or greater

Step 01- Created a virtual Machine on cloud

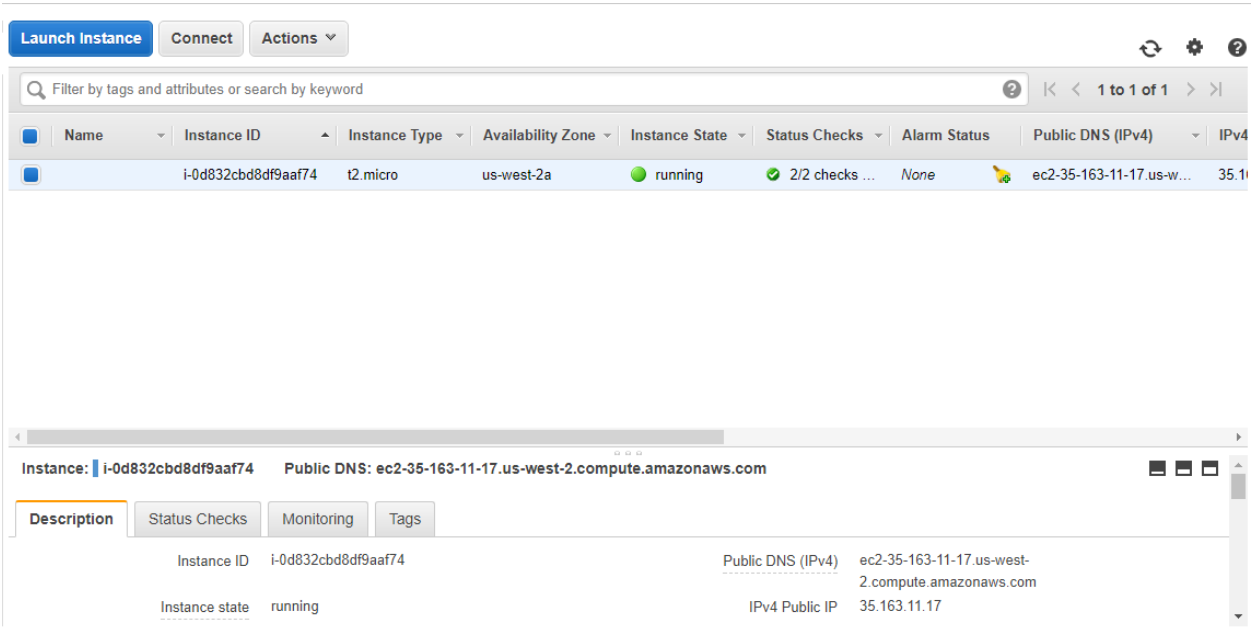


Figure 28- Virtual Machine creation for Hyperledger Composer

Step 02: Created containers and installed Hyperledger Composer

```
curl -sSL https://hyperledger.github.io/composer/install-hlfv1.sh | bash
```

Figure 29- Installing Hyperledger Composer

Step 03: Accessed using http://35.163.11.17:8080

Step 04: Deploy New Business Network

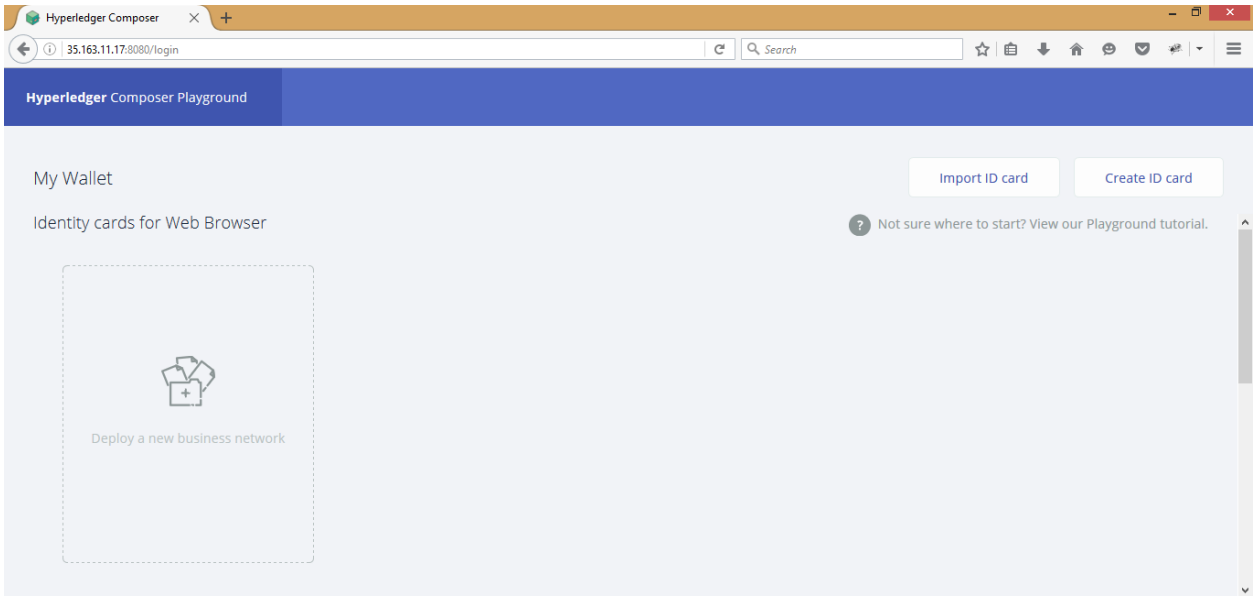


Figure 30- Deploying new Business Network in Hyperledger Composer

Step 05: Enter network details and Deploy

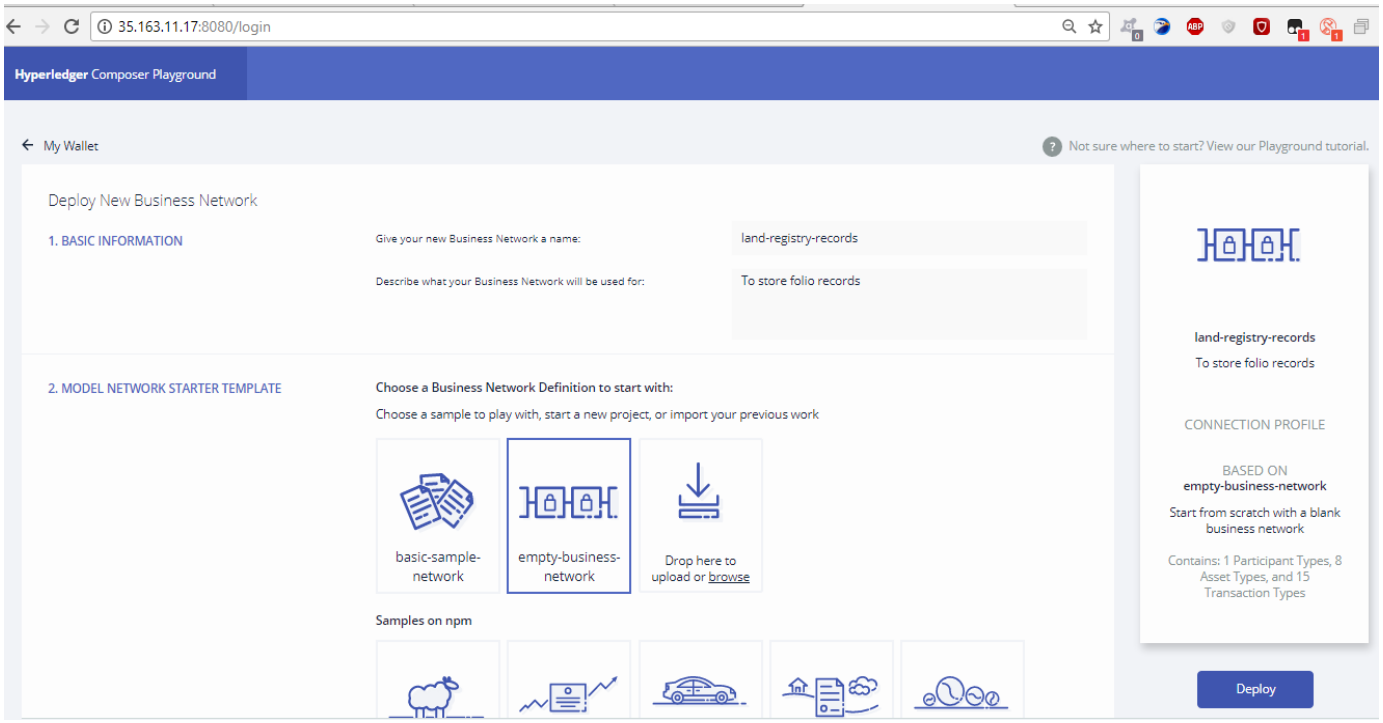


Figure 31- Network Creation in Hyperledger Composer

Step 06: Create model file

```
/**
 * New model file
 */
namespace net.biz.digitalPropertyNetwork

asset FolioRecord identified by DayBookNo {
  o String   DayBookNo
  o String   FolioNo
  o String   DeedNo
  o String   LotNo
  o String   Grantors
  o String   Grantees
  o String   HashValueofDeed
  o String   SignatureOfRegistrationClerk

}
```

Figure 32- Creating Model file in Hyperledger Composer

Step 07: Create script file

Step 08: Create Access control file

ACL File permissions.acl

```
/**
 * New access control file
 */
 rule AllAccess {
     description: "AllAccess - grant everything to everybody."
     participant: "org.hyperledger.composer.system.Participant"
     operation: ALL
     resource: "org.hyperledger.composer.system.**"
     action: ALLOW
 }
```

Figure 33- Creating Access Control file in Hyperledger Composer

Step 09: Add Query files and update Network

Query File queries.qry

```
query Q20{
    description: ""
    statement:
        SELECT net.biz.digitalPropertyNetwork.FolioRecord
            WHERE (DayBookNo=="DayBookNo:100")

}
```

Figure 34- Creating Query File in Hyperledger Composer

Step 10: Create Assets

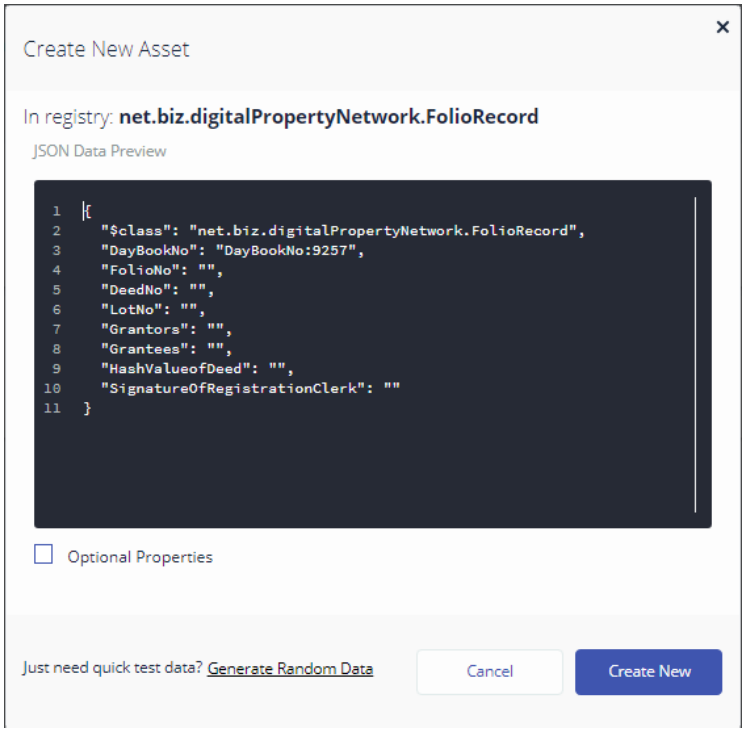


Figure 35- Creating Assets in Hyperledger Composer

4.2.1 Issues in building Hyperledger Composer Prototype

In Hyperledger Composer, when updating the network, it added to the blockchain as a new transaction and that functionality cannot be changed. Therefore, among the transactions containing folio records, Business Network Updating transactions are also added.

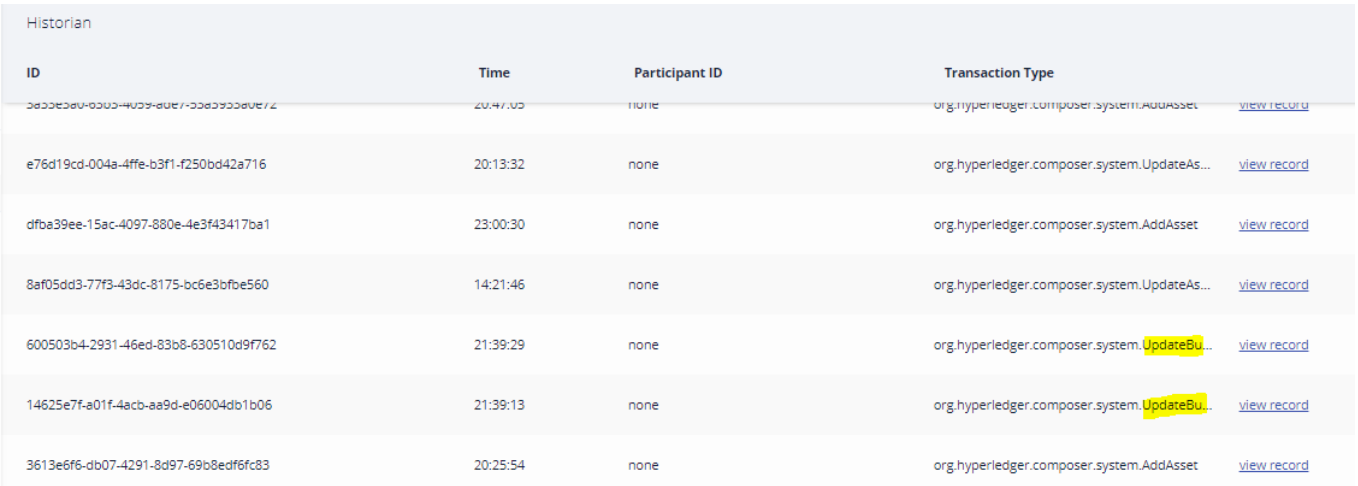


Figure 36- Extra transactions added in Blockchain

In the blockchain, transactions are displayed in transaction wise. Therefore number of transactions that added to a block cannot be detected. That issue is there in the prototype. Hyperledger Composer is not flexible to integrate with web pages. Therefore, the full functionality could not be checked in the prototype.

Chapter 5 - Results and Evaluation

5.1 Prototype evaluation- Multichain

While analyzing the existing problems of the current systems we have identified four major issues that are available in the selected three public data management systems. Namely they are data accessibility concerns, data loss concerns, concerns related to frauds and errors and privacy related concerns. The developed prototype for the electronic health record management system was qualitatively evaluated to verify that it could address those identified issues.

5.1.1 Addressing data manipulation issues

As it is clearly described in previous chapters all three selected systems are vulnerable to data manipulation errors. So we were focusing on using Blockchains in order to restrict those manipulation capabilities. We have utilized the "append only" nature of Blockchains to address the issue.

In order to verify that the data cannot be manipulated in our prototype solution we have attempted to manipulate a transaction with the key value of "Patient_No1"

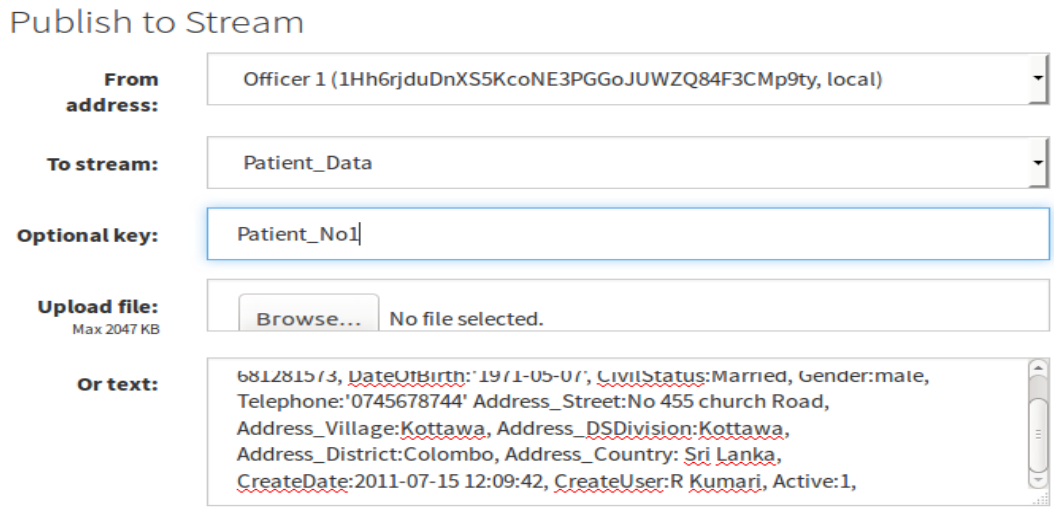


Figure 37- Multichain Evaluation1

As it is displayed in the above picture we have entered the details of a particular patient and in the data section we have entered the UID attribute value as 53. As it is shown in the below

picture it generates a unique txid for that transaction. And when we view the Patient_Data stream it displays only a single record under key value “Patient_No1”

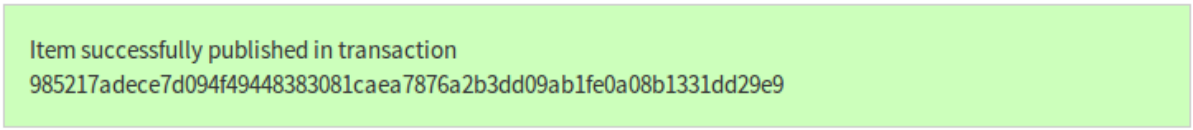


Figure 38- Multichain Evaluation2

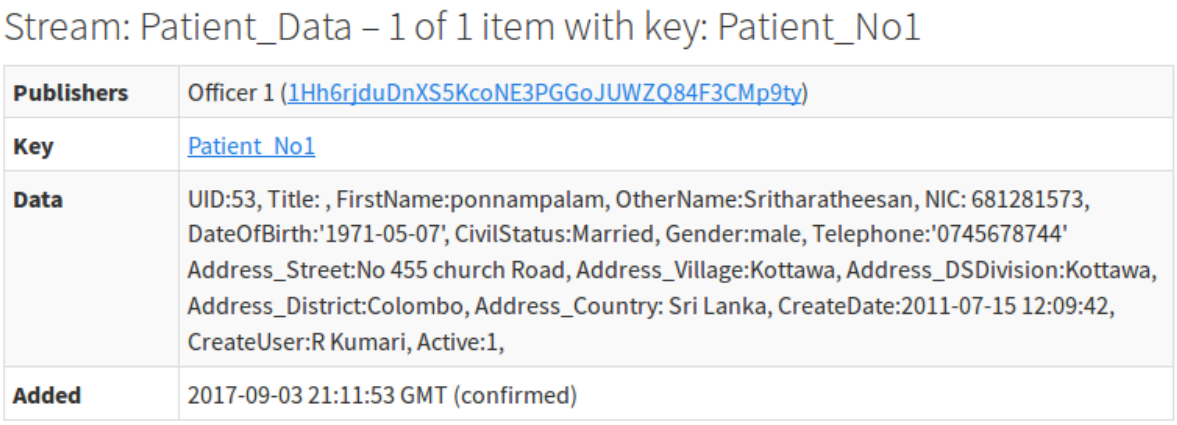


Figure 39- Multichain Evaluation3

In the second attempt we have attempted to initiate another transaction with the key value of “Patient_No1”. And in this we have attempted to change the UID attribute value to 54.

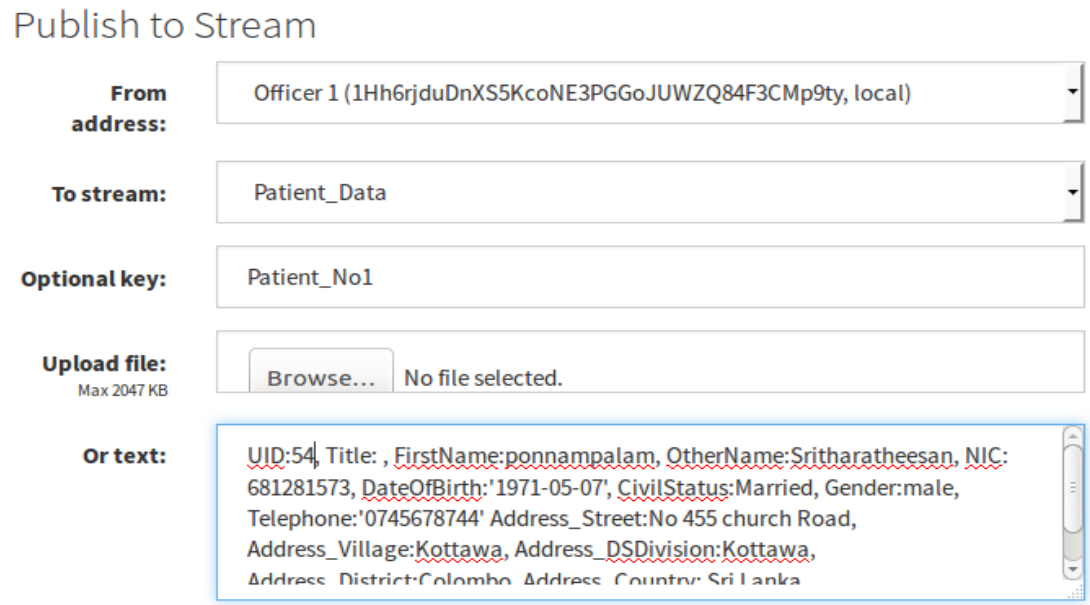


Figure 40- Multichain Evaluation4

As it is displayed below it generates another transaction txid to identify the record separately.

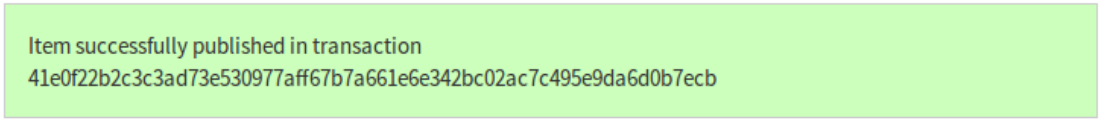


Figure 41- Multichain Evaluation5

And when we view the Patient_Data stream it displays two separate records under key value "Patient_No1" along with their timestamps.

Stream: Patient_Data – 2 of 2 items with key: Patient_No1

Publishers	Officer 1 (1Hh6rjduDnXS5KcoNE3PGGoJUWZQ84F3CMp9ty)
Key	Patient_No1
Data	UID:54, Title: , FirstName:ponnampalam, OtherName:Sritharatheesan, NIC: 681281573, DateOfBirth:'1971-05-07', CivilStatus:Married, Gender:male, Telephone:'0745678744' Address_Street:No 455 church Road, Address_Village:Kottawa, Address_DSDivision:Kottawa, Address_District:Colombo, Address_Country: Sri Lanka, CreateDate:2011-07-15 12:09:42, CreateUser:R Kumari, Active:1,
Added	2017-09-03 21:15:13 GMT (confirmed)

Publishers	Officer 1 (1Hh6rjduDnXS5KcoNE3PGGoJUWZQ84F3CMp9ty)
Key	Patient_No1
Data	UID:53, Title: , FirstName:ponnampalam, OtherName:Sritharatheesan, NIC: 681281573, DateOfBirth:'1971-05-07', CivilStatus:Married, Gender:male, Telephone:'0745678744' Address_Street:No 455 church Road, Address_Village:Kottawa, Address_DSDivision:Kottawa, Address_District:Colombo, Address_Country: Sri Lanka, CreateDate:2011-07-15 12:09:42, CreateUser:R Kumari, Active:1,
Added	2017-09-03 21:11:53 GMT (confirmed)

Figure 42- Multichain Evaluation6

Since it verifies that we cannot replace a record with a particular ID. Since the system users will be given the chance only to append another record with the same ID. This proves that solution prototype is capable to resist the data manipulation attempts.

Furthermore, in the prototype solution there are no option to delete or remove any type of record from the backend or even from the Multichain CLI [61]. Since even if someone really wants to remove some data latterly it cannot be done. Even for a data record, if one attribute value has to be changed only thing what can be done is initiating another transaction along with the new values. The timestamp can be used to identify the record which was added latterly.

5.1.2 Addressing the data loss possibilities

In order to address the data loss possibilities of the prototype; we have utilized the decentralized nature of the blockchain. Since all the records are replicated among available nodes there is no need to maintain separate backup plans or business continuity plans to recover data. In case of a failure of a particular node all the data can be replicated from another node directly. Hence the single point of failure would not directly affect the operations of the system. In the Multichain prototype solution, any node with grant permissions can directly give access to another node which requires access to the data [61]. Since the data loss possibilities are minimized and recovery process from a failure is very simple and effective. Following image displays the permission granting window for a particular node.

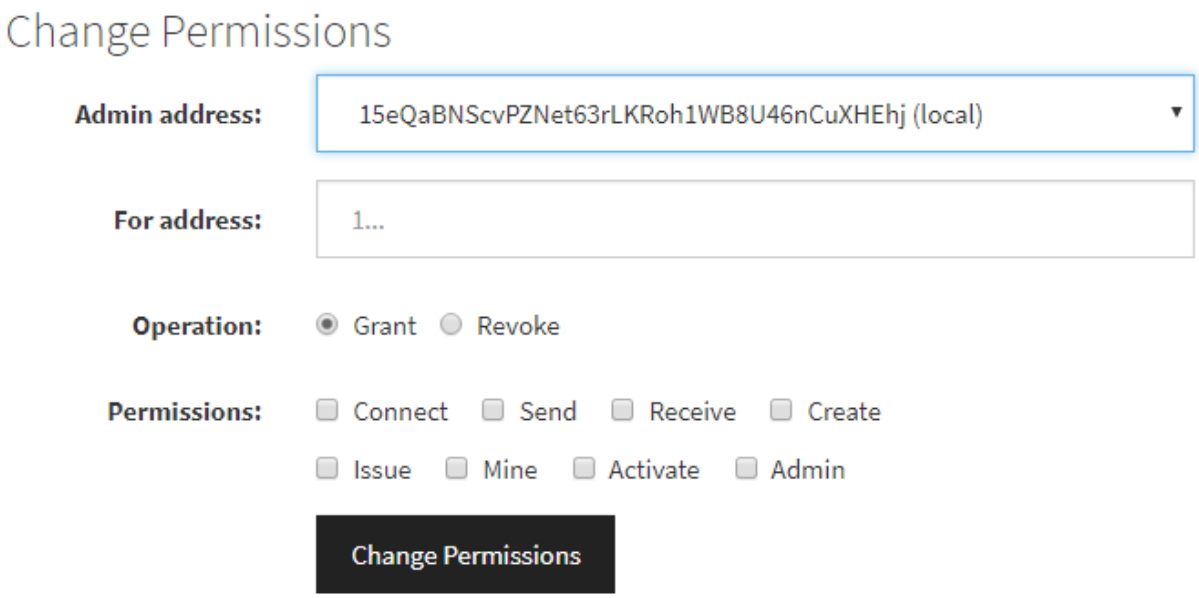


Figure 43-- Multichain Evaluation7

5.1.3 Addressing the data accessibility issues

At the point of initiation of a blockchain in Multichain platform, it reserves a particular port of the server machine and allow the other machines to connect to the blockchain using that specific port. Following image displays the output message it generates at the initiation of a particular blockchain.

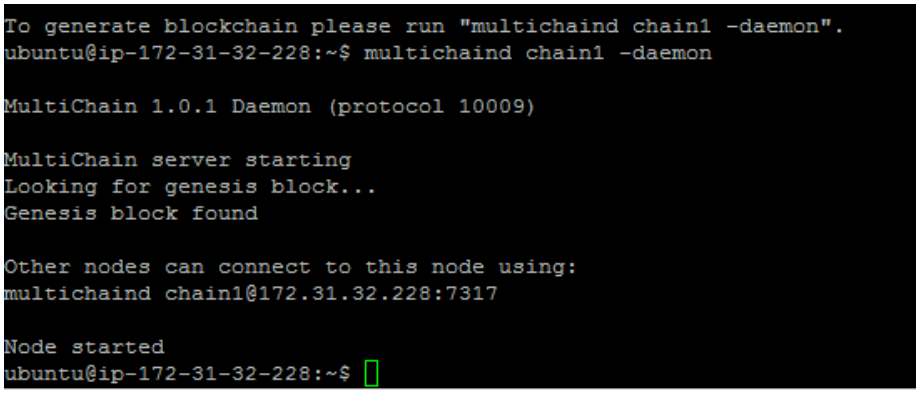


Figure 44- Multichain Evaluation8

Once a particular server wants to connect to the chain it can simply send a request message. If the receiving node have necessary permissions to grant access it can allow the requester to connect to the chain. However it should be noted that even existing nodes with relevant permissions can add new nodes to the chain even without a formal request from the recipient. It can be done using a permission granting window or using the CLI. Following image displays an instance where permissions are granted to a particular node using CLI.

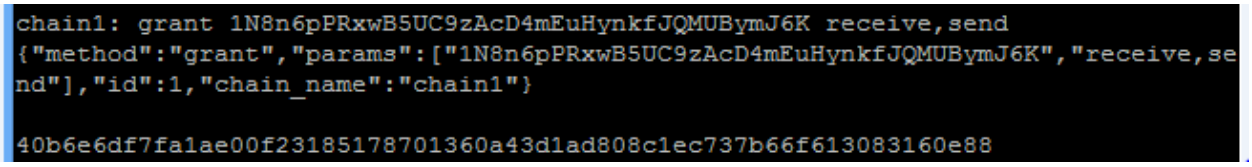


Figure 45- Multichain Evaluation9

Since the design is focused on a private blockchain concept all the nodes in the proposed system are trusted; hence basically the grant permission would be granted to all the nodes in the system.

5.1.4 Addressing the data privacy issues

Furthermore, the privacy issue in the system was addressed by the system design itself. In the design of the electronic health record management system we have used the capabilities of Blockchains along with symmetric cryptography techniques to come up with a privacy preserving mechanism. Hence the prototype is developed according to the design specifications of electronic health data management system.

With the implementation of the prototype solution using Multichain platform; we have verified that all four identified issues in a public data management system can be addressed by a blockchain based solution. Similarly, prototypes can be developed to other two systems as well.

5.2 Prototype Evaluation- Hyperledger Composer

5.2.1 Addressing Data Manipulation Issues

In Hyperledger Composer prototype, 1 Land Title registration certificate is represented as 1 asset. To evaluate the possibility to modify an asset and remain undetected is verified as follows

1. Creating an asset: The transaction ID is dfba39ee-15ac-4097-880e-4e3f43417ba1 is for the folio record


```
    "DayBookNo": "DayBookNo:101",
    "FolioNo": "325",
    "DeedNo": "A57",
    "LotNo": "39",
    "Grantors": "A. N. Weerakoon",
    "Grantees": "A. H. Weerakoon",
    "HashValueofDeed":
"e60de45654c9170d35bc49605959b92cfb13be82f793df381357c3a54e758882"
,
    "SignatureOfRegistrationClerk": "225267890fdhjiuytre"
   }
  ],
  "targetRegistry":
"resource:org.hyperledger.composer.system.AssetRegistry#net.biz.di
gitalPropertyNetwork.FolioRecord",
  "transactionId": "dfba39ee-15ac-4097-880e-4e3f43417ba1",
```


Figure 46-Hyperledger Composer Evaluation1

2. Modify Details in the Asset

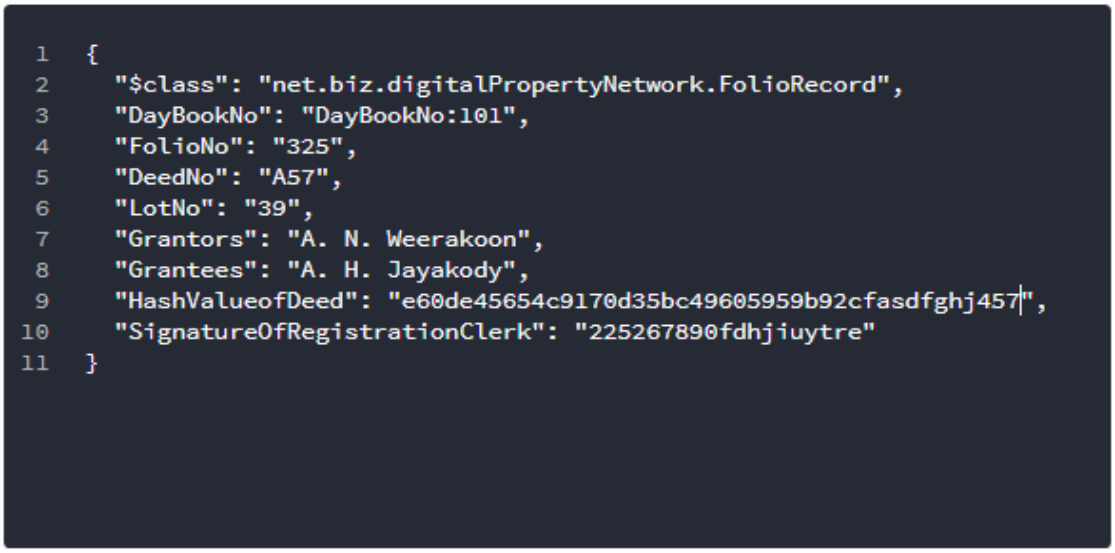


Figure 47-Hyperledger Composer Evaluation2

3. The updated record has transaction ID - e76d19cd-004a-4ffe-b3f1-f250bd42a71

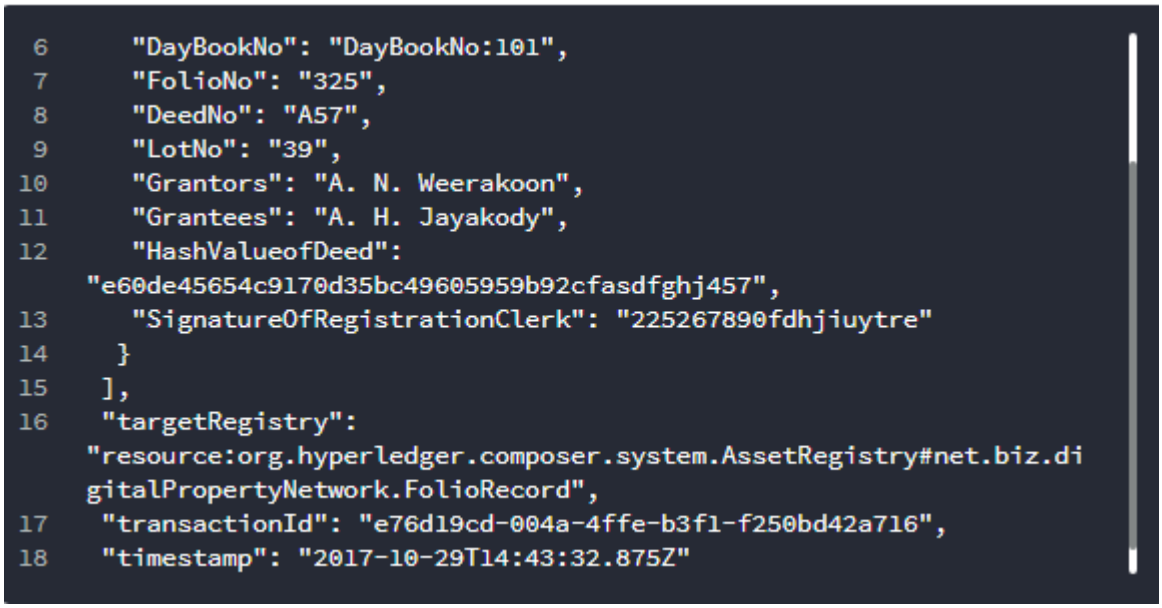


Figure 48-Hyperledger Composer Evaluation3

When checking the ledger, both records do exist with the timestamps.

Figure 49-Hyperledger Composer Evaluation4

Therefore data manipulations can detect in the system. Because the transactions doesn't replace previous ones.

5.2.2 Addressing Data Loss issues

1. Creating a folio record for daybook No 103.

Transaction ID is - 7f4ae9e1-4305-4554-92ff-03e5a5e13e67


```
    "DayBookNo": "DayBookNo:103",
    "FolioNo": "78",
    "DeedNo": "9078",
    "LotNo": "J23",
    "Grantors": "A. D. Perera",
    "Grantees": "S. N. Gamage",
    "HashValueofDeed": "e60de45654c9170d35bc49605959b92cfb13be8",
    "SignatureOfRegistrationClerk": "12erft5632312hos6re4466"
   }
  ],
  "targetRegistry":
"resource:org.hyperledger.composer.system.AssetRegistry#net.biz.digitalPropertyNetwork.FolioRecord",
  "transactionId": "7f4ae9e1-4305-4554-92ff-03e5a5e13e67",
  "timestamp": "2017-10-29T15:21:12.030Z"
}
```


Figure 50-Hyperledger Composer Evaluation5

2. Deleting folio record for daybook No 103

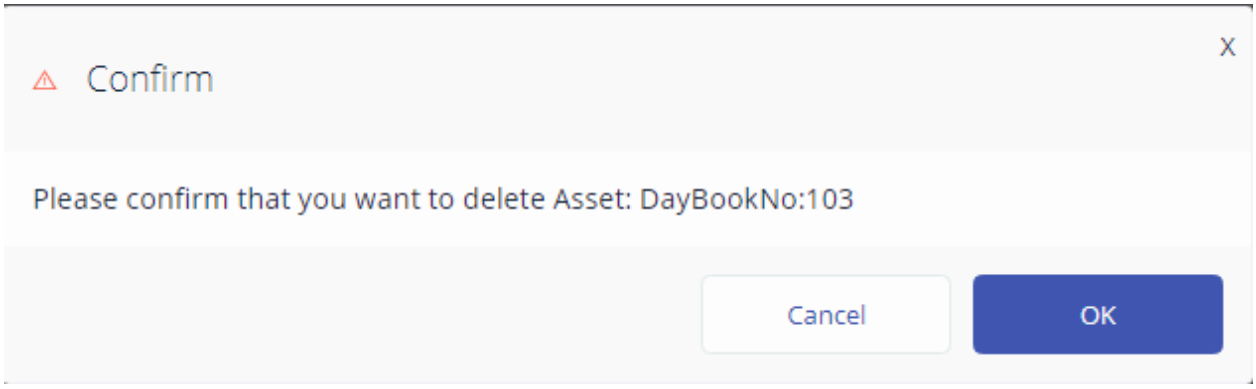
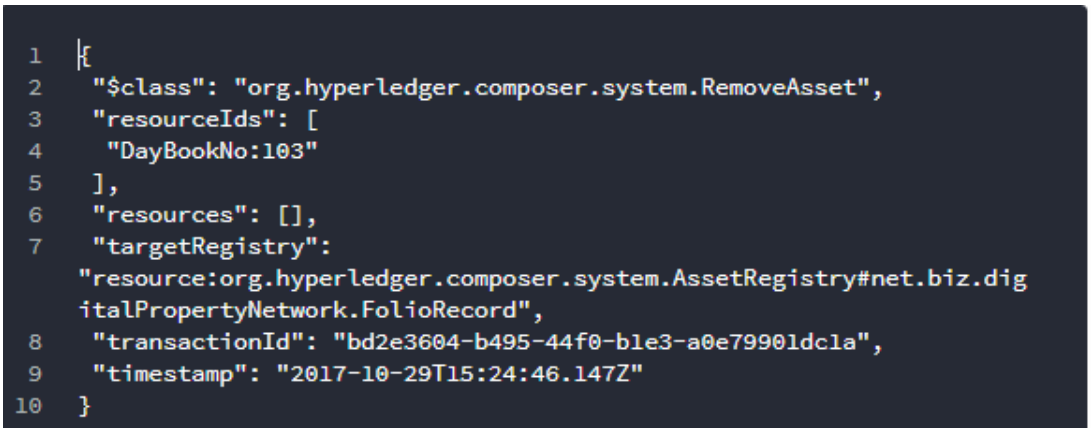


Figure 51-Hyperledger Composer Evaluation6

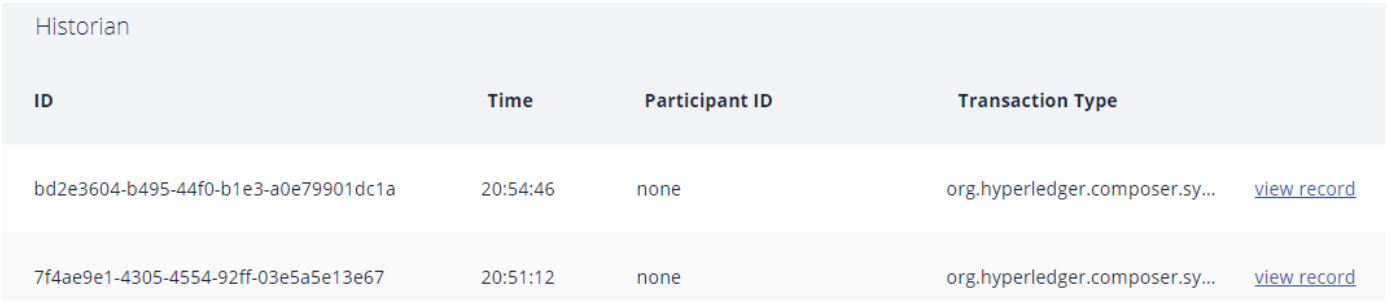
3. Deletion is added as a separate transaction to the ledger



```
{
  "$class": "org.hyperledger.composer.system.RemoveAsset",
  "resourceIds": [
    "DayBookNo:103"
  ],
  "resources": [],
  "targetRegistry":
"resource:org.hyperledger.composer.system.AssetRegistry#net.biz.digitalPropertyNetwork.FolioRecord",
  "transactionId": "bd2e3604-b495-44f0-b1e3-a0e79901dc1a",
  "timestamp": "2017-10-29T15:24:46.147Z"
}
```

Figure 52-Hyperledger Composer Evaluation7

4. When viewing ledger, there are 2 transactions. One for the existed asset and one for the deletion. The data of the deleted transaction did not get disappeared from the ledger



Historian

ID	Time	Participant ID	Transaction Type	
bd2e3604-b495-44f0-b1e3-a0e79901dc1a	20:54:46	none	org.hyperledger.composer.sy...	view record
7f4ae9e1-4305-4554-92ff-03e5a5e13e67	20:51:12	none	org.hyperledger.composer.sy...	view record

Figure 53-Hyperledger Composer Evaluation8

This ensures that there will be no data loss even though the data is deleted in its original place.

Chapter 6 - Conclusions

6.1 Introduction

Computerization of public data records managed by government is done under e-government initiatives of many countries including Sri Lanka. Up To now particular projects came up with different database solutions such as centralized, decentralized, virtual private and cloud databases for storage purposes. However, these solutions have weaknesses where the data loss is still possible and data manipulation is also possible with correct attack. Therefore, there is no single database solution which could address the difficulties in accessibility, data loss and possibility for fraud and error. Blockchain technology which emerged with bitcoin showcased properties that could be used to address these issues that are currently being in question. However it's essential to explore ways on how to actually incorporate Blockchain based mechanisms to the existing public service delivery systems mitigating the issues while considering on the limitations arise with the use of Blockchains. In this research several different ways of using blockchain technology is being analyzed with relevant to the Sri Lankan context which proved to be effective to use as a database solution to create a data management framework for public data which ensure distribution, data availability and data security.

6.2 Conclusions about research questions (aims/objectives)

The main research problem considered in the research is "How to use Blockchain Technology to mitigate data management issues in public data management in Sri Lanka" as mentioned in section 1.2. The research problem further segregated into 4 research questions which comprised the main challenges in public data management namely,

1. Reducing the data accessibility difficulties in public data management systems using blockchain technology
2. Reducing the possibilities of data management frauds and errors using blockchain technology
3. Reducing the data loss possibilities using blockchain technology
4. Privacy Preservation using blockchain technology

From the initial information gathering, these four challenges were identified and they were taken as the objectives to be achieved in the research. Three public data management systems were chosen by considering the e-government initiatives that are already taken. Those selected systems were affected by the four considered challenges mostly. In research approach selected systems were designed using characteristics of blockchain technology to address the challenges. Designs were theoretically evaluated for the ability to address the selected challenges. Abstract prototypes were developed based on the designs and they were qualitatively evaluated for the considered four criteria of challenges.

Qualitative evaluation passed the all four criteria considered although few limitations were recognized. However evaluation of the prototypes were not precise due to the limitations in the platforms used to build prototypes. Since blockchain is a complex concept, building a blockchain from scratch is not possible within the research time period. Therefore existing two platforms were used which matched the requirement. Number of existing open source platforms are less and their customization ability was also a bit inflexible

6.3 Limitations

When designing the selected systems, few limitations were recognized.

6.3.1 Limitations in Birth Marriage Death Certificate Management System Design

One of the main limitation with regard to design of the Birth, Marriage, Death certificate Management system design is the concerns associated with the adoption of the introduced mobile wallet based mechanism. Sine we are using the currently existing system as the foundation for developing the blockchain based mobile wallet mechanism the solution presented through the system is a value adding extension to the current system. Therefore a question is there whether the people are motivated to go through the registration procedure of the mobile wallet in order to obtain their own digital certificate. However since we proposed having web portals for third party organizations in order to carry out the verification of these different type of certificates there is a tendency that these external organization will create a requirement of owning a mobile wallet with relevant digital certificates with each individual

since it's more convenient for them as well as it will lead to correct validation of the documents eliminating frauds. So that the common citizens are encouraged to involve with service.

Another limitation that we came across when designing the system is the storage capacity of a particular block and the effect it has on the mining function. As mentioned in the Chapter 3, since the image size exceed the size of a block transaction it lead us to go for an alternative approach where the scanned images of the documents are stored in a separate database while only the hash values are stored in the blockchain for supporting the verification process.

However, during the research period, with the time restrictions we only build two prototypes for the other two systems, without focusing in this design, because of the fact that this design involves many stakeholders as well as different technological components to full build a working prototype. And with considerations on the research scope and the time limitations we decided only to build two working prototypes for the other two systems since our main intention through our research is to analyze the characteristics of Blockchain which makes it suitable for applying in the public service delivery systems domain. And since the Blockchain concept is similar to all the three system, the characteristics which are shown by the prototypes of other two system will also be applicable for the Blockchain in the proposed design of this particular solution as well.

6.3.2 Limitations in Land Title Management System Design

In Land Title Management design, the blockchain is used as a verification repository where it has only the data which can point out the owner of a particular land. All Deed documents and other folio data are stored in the traditional Relational Database. Therefore, if backups are not kept, those data may get destroyed in a failure. Only the ownership details will be remained. Whole set of data including the Deed document cannot be added to the blockchain because then the mining would be more expensive.

The platform used to build the prototype is the Hyperledger Composer [48]. However due to the limitations in customization of the platform, the prototype we developed was not exactly mapped with the design. Since the Hyperledger Composer provides an executable which cannot be integrated into a single system with rest of data in the database, evaluation of

full functional system was not achieved. In Design, we have declared the number of folio records that can go to one block. However, in Hyperledger Composer, display is in transaction wise and blocks cannot be viewed. Therefor number of folio records that fit into one block could not be evaluated. In design, we theoretically suggested that mining should be done in proof of work concept [25]. However, the mining is not visible in the prototype and it couldn't be evaluated for the Land Title Management prototype.

6.3.3 Limitations in eHealth Record Management System Design

One of the major concerns of the proposed blockchain solution is that it may not suitable for all the clinical scenarios. The system is designed in a way that the patients can obtain the medicine through hospitals without exposing their personal identities. However, the hiding the personal identities may not be a requirement for all the clinical situations. Furthermore, it may be not suitable in some clinical situations. Especially in the instances such as Emergency Treatment Units hiding the patient's identities would be problematic. Hence the proposed system is well suited only for the clinical instances where protecting patient's identity is a major concern.

Another major concern in the proposed eHealth Record Management System is the maintenance of the patient's symmetric keys. In order to achieve complete privacy; in the proposed system the symmetric key of a particular patient is only kept by that particular patient. If the system is designed in a way that it could maintain list of symmetric keys along with the patient IDs in a database; then again, the database administrator will be able to see the keys of all the patients. However, in the proposed system even the database administrators of the medical database will not have opportunity to access the medical records since they don't have the access to symmetric keys of patients. In an instance where the patient loss his/her symmetric key there will be no proper way to recover it. This problem is mainly prominent in the scenarios where the patient use the proposed patient card. If the patient is using the mobile application, then the user will have some recovery options to remember the key. However, in the typical patient card scenario once the card is lost there is no proper mechanism to recover it from the system. Hence there is a direct conflict between achieving privacy and the continuity of the system.

Furthermore, in the proposed system for eHealth Record Management System the blockchain will only maintain the identity related personal details of the patients. The critical information such as diagnosis records, medication records will not be stored in the blockchain. Hence that medical information only resides in the medical database and won't be replicated among all the nodes of the blockchain. In case of a database failure the identity related details would be secured in the blockchain and the identities of the patients will be secured. Still the medical staff will not get the chance to operate completely depending on blockchain since part of the data is stored in database.

6.4 Implications for further research

The blockchain solutions can be further scale into a single Blockchain for the Sri Lankan government where the critical information relevant to different public service delivery systems will be resides within a unique stream in Blockchain [60]. And also the wallet concept that we are presented in the Birth Marriage Death Certificate Management solution can be incorporated with the Land Title Management System where a single wallet may able to hold all real estate ownership for a particular person. If such wallet can be incorporated in Land Title Management, real estate transactions can be enabled and land Title token can be converted into a tradable object, like a bitcoin. Furthermore, for the designs that we have presented in the research incorporate proof-of-work mining concept, where there are many alternatives for different mining algorithms with their own pros and cons. There is a future work opportunity in identifying or developing a specific mining algorithm that will suit more to the requirements and the infrastructure capabilities of the government sector. And also one of the limitations we faced was the size of a particular Block in the Blockchain and the limitations of it. Therefore research opportunities are there to introduce a flexible Block size Blockchain or a Blockchain architecture where the Block size can be vary according to the transactions that are being recorded.

Chapter 7 - References

[1]"The Government Information Center", Gic.gov.lk, 2017. [Online]. Available: http://www.gic.gov.lk/gic/index.php?option=com_info&id=355&task=info&lang=en. [Accessed: 12- Mar- 2017].

[2] 2017. [Online]. Available: http://www.statistics.gov.lk/Abstract2014/CHAP3/3.19.pdf. [Accessed: 12- Mar- 2017].

[3]SUNDAY TIMES, "Busting of fake kachcheri at Hulftsdorp turning out NICs raises many questions", 2016.

[4]"Information and Communication Technology Agency | ICTA", Icta.lk, 2017. [Online]. Available: https://www.icta.lk/current-projects/. [Accessed: 04- May- 2017].

[5] "Database Auditing: Security Considerations", Docs.oracle.com, 2017. [Online]. Available: https://docs.oracle.com/cd/B19306_01/network.102/b14266/auditing.htm#i1008322. [Accessed: 20- May- 2017].

[6]"Blockchain", Blockchain.com, 2017. [Online]. Available: https://www.blockchain.com/. [Accessed: 19- Feb- 2017].

[7]S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 1st ed. 2008.

[8]M. Swan, Blockchain BLUEPRINT FOR A NEW ECONOMY, 1st ed. O'Reilly Media, 2015.

[9] G. Vashakidze, "One-Stop-Shop Public Service Delivery Model: the Case of Georgia," United Nations Dev. Program. Reg. Hub Civ. Serv. Astana, no. January, 2016.

[10]S. Bhatnagar, "Public service delivery: Role of information and communication technology in improving governance and development impact," ADB Econ. Work. Pap. Ser., no. 391, 2014

[11] A. Prakash and R. De', "Importance of development context in ICT4D projects," Inf. Technol. People, vol. 20, no. 3, pp. 262–281, 2007.

[12]Electronic Integration of BHOOMI with Stakeholders, Karnataka, 1st ed. National Informatics Centre & Revenue Department, Government of Karnataka, 2014.

[13]P. ATTYGALLE and I. MAHANAMA, INNOVATIONS IN LAND INFORMATION RECORDING, MANAGEMENT AND UTILIZATION IN SRI LANKA, 1st ed. 2016.

[14]"Report of Committee On Computerisation of Land Records", Government of India Ministry of Rural Development Department of Land Resources, 2005.

[15]"Data Breach Statistics by Year, Industry, More - Breach Level Index", Breach Level Index, 2017. [Online]. Available: http://breachlevelindex.com/. [Accessed: 09- May- 2017].

[16] B. Sangeetha, E. Saranya, and G. Saranya, "A NOVEL FRAMEWORK FOR SECURE SHARING OF PERSONAL HEALTH RECORDS (PHR) IN CLOUD COMPUTING," vol. 2, 2015

[17] P. Patel and A. Buchade, "Survey on Achieve Privacy Preserving using Multi-Key Approach in Cloud Environment," vol. 1, no. 5, pp. 8–12, 2014

[18]G. Kong and Z. Xiao, "Protecting privacy in a clinical data warehouse", Health Informatics Journal, vol. 21, no. 2, pp. 93-106, 2014.

[19]D. Floyd, "51% Attack", Investopedia, 2017. [Online]. Available: http://www.investopedia.com/terms/1/51-attack.asp. [Accessed: 20- May- 2017].

[20]"Applications of Blockchain Technology to Banking and Financial Sectors in India", Institute for Development and Research in Banking Technology, 2017.

[21]"Genesis block - Bitcoin Wiki", En.bitcoin.it, 2017. [Online]. Available: https://en.bitcoin.it/wiki/Genesis_block. [Accessed: 14- Apr- 2017].

[22]"Block - Bitcoin Wiki", En.bitcoin.it, 2017. [Online]. Available: https://en.bitcoin.it/wiki/Block. [Accessed: 14- Apr- 2017].

[23]W. root, "What is the Merkle root?" Bitcoin.stackexchange.com, 2017. [Online]. Available: https://bitcoin.stackexchange.com/questions/10479/what-is-the-merkle-root. [Accessed: 14- Apr- 2017].

[24]"Introduction — Sawtooth latest documentation", Intelledger.github.io, 2017. [Online]. Available: https://intelledger.github.io/introduction.html. [Accessed: 18- Sep- 2017].

[25]F. Zhang, R. Escriva, and R. Van Renesse, "REM : Resource-Efficient Mining for Blockchains."

[26]D. Guarda, "Top Blockchain Possible Applications", Intelligent Head Quarters, 2017. [Online]. Available: https://www.intelligenthq.com/innovation-management/some-of-Blockchains-possible-applications/. [Accessed: 04- May- 2017].

[27]G. Foroglou and A. L. Tsilidou, "Further applications of the Blockchain," Conf. 12th Student Conf. Manag. Sci. Technol. Athens, no. MAY, pp. 0–8, 2015.

[28] ZahraGhaffari, "On the application areas of Blockchain," 2016.

[29]P. Boucher, “How Blockchain technology could change our lives,” Eur. Parliam. Researcg Serv., 2017.

[30]Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, “Blockchain Challenges and Opportunities: A Survey,” no. December 2016, 2017.

[31] Working Group on Intellectual Property, “HOW BLOCKCHAINS CAN SUPPORT , COMPLEMENT , OR SUPPLEMENT INTELLECTUAL PROPERTY” pp. 0–24

[32]S. Shinner, "Blockchain technology and IP", Taylorwessing.com, 2017. [Online]. Available: https://www.taylorwessing.com/download/article-Blockchain-technology-and-ip.html. [Accessed: 06- May- 2017].

[33]"A Secure Model of IoT with Blockchain - OpenMind", OpenMind, 2017. [Online]. Available: https://www.bbvaopenmind.com/en/a-secure-model-of-iot-with-Blockchain/?utm_source=views&utm_medium=article06&utm_campaign=MITcompany&utm_content=banafa-jan07. [Accessed: 04- May- 2017].

[34]"What Blockchain Can Do for IoT - DZone IoT", dzone.com, 2017. [Online]. Available: https://dzone.com/articles/what-Blockchain-can-do-for-the-internet-of-things. [Accessed: 04- May- 2017].

[35]M. Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?", SSRN Electronic Journal.

[36]"Can Blockchain spark a government services revolution? -- GCN", GCN, 2017. [Online]. Available: https://gcn.com/articles/2016/09/27/Blockchain-government-services-revolution.aspx. [Accessed: 05- May- 2017].

[37]S. Ølnes, BEYOND BITCOIN Public Sector Innovation Using the Bitcoin Blockchain Technology, 1st ed. 2014.

[38] A. Linn and M. B. Koo, “Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research,” pp. 1–10, 2014

[39] [G. Zyskind, O. Nathan, and A. 'sandy' Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” 2015 IEEE Security and Privacy Workshops, 2015.]

[40] [K. Biswas and V. Muthukkumarasamy, “Securing Smart Cities Using Blockchain Technology,” 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016.].

[41]"Whitepaper – Bitland", Bitland.world, 2017. [Online]. Available: http://www.bitland.world//wp-content/uploads/2016/03/Bitland_Whitepaper.pdf. [Accessed: 11- Apr- 2017].

[42]Medium. (2017). Blockcerts-An Open Infrastructure for Academic Credentials on the Blockchain. [online] Available at: https://medium.com/mit-media-lab/blockcerts-an-open-infrastructure-for-academic-credentials-on-the-blockchain-899a6b880b2f [Accessed 16 Dec. 2017].

[43]Blockcerts. (2017). Blockchain Certificates. [online] Available at: https://www.blockcerts.org/guide/ [Accessed 16 Dec. 2017].

[44]A. Schaub, R. Bazin, O. Hasan, and L. Brunie, "A Trustless Privacy-Preserving Reputation System," ICT Systems Security and Privacy Protection IFIP Advances in Information and Communication Technology, pp. 398–411, 2016]

[45] [J. Herbert and A. Litchfield, "A Novel Method for Decentralised Peer - to - Peer Software License Validation Using Cryptocurrency Blockchain Technology," 38th Australas. Comput. Sci. Conf. (ACSC 2015), no. January, pp. 27–30, 2015]

[46] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu, "The Blockchain-Based Digital Content Distribution System," 2015 IEEE Fifth Int. Conf. Big Data Cloud Comput., pp. 187–190, 2015.

[47] G. Greenspan, "MultiChain Private Blockchain — White Paper," pp. 1–17, 2013.

[48]"Introduction | Hyperledger Composer", Hyperledger.github.io, 2017. [Online]. Available: https://hyperledger.github.io/composer/introduction/introduction.html. [Accessed: 29- Aug- 2017].

[49] P.Dissanayaka, M.Wanigasekara "BMD Project status in Thimbirigasyaya Divisional Secretariat", Thimbirigasyaya Divisional Secretariat, 2017.

[50]"Mobile Wallet Basics – Wells Fargo", Wellsfargo.com, 2017. [Online]. Available: https://www.wellsfargo.com/mobile-payments/mobile-wallet-basics/. [Accessed: 18- May- 2017].

[51] D. Seneviratne "Status of eLand Registry System", Land Registry Office, 2017

[52] "hhimsv2", Hhims.org, 2017. [Online]. Available: http://www.hhims.org/. [Accessed: 15- Mar- 2017].

[53]S. Rathnayake, "Hospital Health Information Management System (HHIMS) V 2.0", 2015.

[54] K.Wickramasuriya,"Hospital Health Information Management System (HHIMS) project status in Sri Lanka", ICTA - Colombo 05, 2017.

[55]"Guides: The Hippocratic Oath and others: Oaths", Hslmcmaster.libguides.com, 2017. [Online]. Available: http://hslmcmaster.libguides.com/c.php?g=306726&p=2044095. [Accessed: 06- Oct- 2017].

[56]L. A. Linn, “Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research,” pp. 1–10, 2014.

[57]"Types of Blockchain — Public, Private and Permissioned", Darwin Labs, 2017. [Online]. Available: https://blog.darwinlabs.io/types-of-blockchain-public-private-and-permissioned-5b14fbfe38d4. [Accessed: 18- Sep- 2017].

[58]"What is the Bitcoin Block Size Debate and Why Does it Matter?", CoinDesk, 2017. [Online]. Available: https://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter. [Accessed: 18- Sep- 2017].

[59]"Storing document/file in blockchain", Ethereum.stackexchange.com, 2017. [Online]. Available: https://ethereum.stackexchange.com/questions/7842/storing-document-file-in-blockchain. [Accessed: 18- Sep- 2017].

[60]Multichain.com. (2017). MultiChain data streams | MultiChain. [online] Available at: https://www.multichain.com/developers/data-streams/ [Accessed 16 Dec. 2017].

[61]G. Greenspan, "Blog | MultiChain | Open source blockchain platform", Multichain.com, 2017. [Online]. Available: https://www.multichain.com/blog/. [Accessed: 18- Jun- 2017].