



**BLOCKCHAIN TECHNOLOGY FOR PRESERVING DIGITAL
LAND RECORDS**

Case of Addis Ababa City Administration

A Thesis Presented

by

Sara Ayele

to

The Faculty of Informatics

of

St. Mary's University

**In Partial Fulfillment of the Requirements
for the Degree of Master of Science**

in

Computer Science

March, 2021

ACCEPTANCE

BLOCKCHAIN TECHNOLOGY FOR PRESERVING DIGITAL LAND RECORDS

By

Sara Ayele

**Accepted by the Faculty of Informatics, St. Mary's University, in partial
fulfillment of the requirements for the degree of Master of Science in
Computer Science**

Thesis Examination Committee:

Michael Melese (Ph.D.)

Internal Examiner

Temtim Assefa (Ph.D.)

External Examiner

Getahun Semeon (Ph.D.)

Dean, Faculty of Informatics

February, 2021

DECLARATION

I, the undersigned, declare that this thesis work is my original work, has not been presented for a degree in this or any other universities, and all sources of materials used for the thesis work have been duly acknowledged.

Sara Ayele

Full Name of Student

Signature

Addis Ababa

Ethiopia

This thesis has been submitted for examination with my approval as advisor.

Getahun Semeon (Ph.D.)

Full Name of Advisor

Signature

Addis Ababa

Ethiopia

February, 2021

Acknowledgment

First and foremost, I would like to thank the Almighty God for giving me the strength to complete this thesis and help me in such tough times in all directions of my life.

I would like to express my gratitude to my supportive advisor Dr. Getahun Semeon for believing in me from the beginning, all his guidance, encouragement and advice throughout the time gave me the confidence to accomplish this work.

I would like to thank all the staffs of the AALHRIA and my friends for their valuable supports and standing by me in all the difficult moments especially Tade you are the reason why I am here.

Finally, I am very thankful to my father Ato Ayele Gemechu (አንታዬ) and my mother W/ro Zenebech Senbeta (አዬ) for all the love and support you gave me and all of the rest of my families in one or the other way you brought me to a success in my academic endeavor. Thank You!!!

Contents

ACKNOWLEDGMENT	I
LIST OF ACRONYMS	V
LIST OF FIGURES	VI
LIST OF TABLES	VII
ABSTRACT	VIII
1. INTRODUCTION	1
1.1 Background.....	1
1.2. Statement of the Problems	2
1.3. Research Questions	4
1.4. Objectives of the study	4
1.4.1. General objective	4
1.4.2. Specific objectives	4
1.5. Methodology.....	5
1.6. Scope of the study	5
1.7. Significance of the study	5
1.8. Limitation of the study	6
1.9. Organization of the paper	6
2. LITERATURE REVIEW AND RELATED WORKS	7
2.1. INTRODUCTION	7
2.1.1. What is blockchain?	7
2.1.2. Essential Characteristics Related with Blockchain	9
2.1.3. Core Components of Blockchain and how they work.....	12
2.1.4. Block formation Phases of Operation.....	15
2.1.5. Block acceptance and chain update	18
2.1.6. Blockchain Types	19

2.1.7. A brief history of Blockchain	22
2.1.8. Evolution of Blockchain Generations	24
2.1.9. Records and Its preservation	26
2.1.10. Blockchain and Land Record Preservation	27
2.1.11. Features of Blockchain technology in land record management.....	30
2.2. RELATED WORKS	31
3. RESEARCH METHODOLOGY.....	35
3.1 Introduction	35
3.2 Research Design	35
3.3 Research Approach.....	35
3.4 Qualitative Research Approach.....	36
3.5 Research Context.....	36
3.6 Source of Data	37
3.7 Data Collection Tools.....	37
3.7.1 Document Analysis.....	37
3.7.2 Interview	38
3.7.3 Observation Technique	40
3.7 Method of Data Analysis.....	41
3.8. Research Validity and Reliability.....	41
3.8.1 Validity	41
3.8.2 Reliability.....	41
3.9 Design Science Research Approach	41
4. SYSTEM ANALYSIS AND DESIGN	45
INTRODUCTION	45
4.1 SYSTEM ANALYSIS.....	45
4.1.1 Overview of the existing System	45

4.1.2 Proposed System.....	48
4.1.3 Actors of the System.....	49
4.1.4 Use Case Diagram.....	50
4.1.5 Use Case Description.....	50
4.1.6 Sequence Diagram	52
4.2 SYSTEM DESIGN.....	54
4.2.1 Proposed System Architecture.....	54
4.2.2 Main Components of the Prototype	56
5. IMPLEMENTATION AND EVALUATION	58
5.1 IMPLEMENTATION	58
5.1.1The System Development Environment	58
5.1.2. Setup and Deployment.....	59
5.1.3 Prototype Demonstration	63
5.2 Testing	67
5.3 Evaluation.....	69
6. CONCLUSION AND RECOMMENDATIONS	71
6.1. Conclusion.....	71
6.2 Recommendations	72
REFERENCES	73
APPENDICES.....	77

List of Acronyms

FDRE - Federal Democratic Republic of Ethiopia

IPRIA - Immovable Property Registration and Information Agency

AALHRIA - Addis Ababa City Administration Land Holding Registration and Information Agency

AA-LIS - Addis Ababa Land Information System

ICT - Information and Communication Technology

RECS - Real Estate Cadastral System

RPRS - Real Property Registration System

DLT - distributed ledger technology

DApp – Decentralized Application

IDE –Integrated Development Environment

IPFS - Inter Planetary File System

DSR - Design Science Research

AES - Advanced Encryption Standard

GIS - Geographical Information System

API- Application Programming Interface

List of Figures

Fig. 2-1 Vital blockchain characteristics.....	11
Fig. 2-2 Sample Block Structure	17
Fig.2-3 Sample blocks in blockchain.....	19
Fig.2- 4 Historical evolution of blockchains.....	26
Fig. 3-1 General design cycle of DSR (Kuechler and Vaishnavi).....	42
Fig. 4-1 Use case diagram of the system	50
Fig. 4-2 Sequence diagram for the prototype	53
Fig. 4-3 Architecture of the proposed prototype	55
Fig.4-4 Interaction among main components	57
Fig. 5-1 Available accounts & addresses.....	60
Fig. 5-2 Sample Account	61
Fig. 5-3 Login and home page of the DApp.....	64
Fig. 5-4 Registering a record in blockchain.....	65
Fig 5-5 View Record page.....	65
Fig. 5-6 Attaching the scanned record.....	66
Fig. 5-7 Block information.....	66
Fig 5-8 Remix unit test result.....	68
Fig. 5-9 Deploying on Ropsten network.....	69

List of Tables

Table 3-1 Description of participants	40
Table 4-1 Actors of the system.....	49
Table 5-1 Development tools used	58
Table 5-2 summary of respondents' score.....	70

Abstract

Preservation of records in a secure way is the most important issue in any city circumstance especially when it comes to land record it becomes a more significant one. A secured land records will make the institution strong with an effective and accountable working environment. The main objective of this thesis is to explore and show how to ensure the security of the Land Records using Blockchain Technology. This study used a mixed method research approach. The security problem in the existing system which is mainly security of records is identified using interview, observation and document analysis. Based on the problems identified a System is proposed and a prototype is developed that integrates newly emerging technology Ethereum Blockchain and Interplanetary File System (IPFS) with a DApp that is developed for users to interact. The functionality is managed by the smart contract. The prototype is capable of registering a record; attach the necessary image files and also viewing the registered records. The hash of registered record and the attached image is placed as transaction on the blockchain. The records are immutable and times stamped and are only accessible by the authorized users. Generally, this thesis explored and demonstrated the potential of the blockchain in addressing the security problems and preservation of records.

Key words: Blockchain, Land records, Smart contracts, Ethereum, IPFS, DApp

CHAPTER ONE

1. INTRODUCTION

1.1 Background

As article 40(3) of the FDRE constitution succinctly puts, land is a common property of the Nations, Nationalities and Peoples of Ethiopia and shall not be subject to sale or to any other means of exchange. The same ideal is reiterated under article 89(4) of the same constitution. From the above constitutional benchmarks, one can easily understand the role that land plays in the political economy of this country. [8]

Be this as it may, due to lack of institutional, legal and technological frameworks towards the effective and efficient utilization of land; and the rampant rent seeking behavior that abounded so far, this scarce resource has been abused and in so far as building a developed property market is concerned, contributed a trivial role. [7]

The city of Addis Ababa, the capital of Ethiopia, began implementing its first land registration system in 1907. Since then land registration and its respective services have gone through many diverse and unstable institutional and organizational arrangements. As a result over time the system had become increasingly unmanageable, particularly with the accelerated urbanization of Addis Ababa over the previous two decades. [7, 8]

Addis Ababa City Government Proclamation No. 22 /2010 established the Immovable Property Registration and Information Agency (IPRIA) the name changed to Addis Ababa City Administration Land Holding Registration and Information Agency (AALHRIA) and came into force in June 2010. It declared that the agency to be a legal entity headed by a board accountable to the city manager. In addition head office of the agency was to retain and still retains offices in each sub-city. [7]

The objectives of the agency were defined as

- Ensuring the implementation of a secure, reliable, trustworthy and efficient cadaster information system (AA-CADIS)
- Delivery of immovable property information from AA-CADIS and Addis Ababa Land Information System(AA-LIS)
- Support of land management, land use planning and property valuation
- Fostering the economic development of the City of Addis Ababa

- Supply property information to the city's citizens and the private sector

Since the establishment of the agency many actions has been performed to use application of Information and Communication Technology (ICT) one of them is maintaining a digital archive system to enhance the service delivery also trust of the employees in using the system within the rules of the existing law.

Most of the works attempts to manage the land records using the client server based platforms which is actually being implemented in the agency also. The emerging block chain technology having this interesting feature of immutable, greater transparency enhanced security and traceable features are initiating governments around the world to implement the decentralized technology in many areas.

Blockchain brings many advantages encompassing provenance, accountability, traceability and transparency of the transactions stored in the ledger. It provides a fully decentralized root of trust avoiding central authorities, thereby facilitating trust across initially non-trusted or unknown stakeholders and users. The decentralized nature makes highly difficult to alter transaction history. In addition, blockchain transactions are stored in a fully decentralized peer to peer network, which replicates data storage, thereby disabling potential data loss. Among many platforms available in the blockchain here the potential of Ethereum blockchain that enables the deployment of smart contracts and decentralized applications (DApps) is explored and presented in preserving digital land records.

1.2. Statement of the Problems

Organizations are recognizing the critical benefit that can be gained from emerging information systems and started to adopt Information System to automate their business process.

Addis Ababa City Administration Land Holding Registration and Information Agency is currently using three systems those are RECS (Real Estate Cadastral System) which register the spatial data, RPRS (Real Property Registration System) for non-spatial data and the archive system which store all the paper-based files of each owner detail of land history digitally.

The two registration system are being used effectively and about 80,000 parcels have been registered and it is showing progress to the service delivering sector and in the near future

there's a plan to making the registering online. Also about 95,000 owners' documents have been digitized for the archive system.

The current archive system of the agency has been designed in order to the address these issues to:-

- Minimize the time which lasts to locate, find or retrieve land ownership file
- Decrease loosing, dislocating and confusing records
- Keep the record in a secure mode
- Make records accessible in a day to day agency activities and generating a required report on time.

Even though the existing system try to address the desired issue by focusing on designing a system to automate the manual system and store the digitized records of the owners it has a security gaps that prohibit the system to be used further more efficiently. The only security mechanism used in the system is only user management by giving them their own privileges. Any user with the privilege of manipulating a record can perform the action without any restriction. It can only be detected after the action is performed from the database log file. There is a security threats on the integrity of the records because it has no mechanism for detection or restriction on abuse of records which lead to inadequate decision making while giving services for the customers that will make the agency untrusted and it exposes the services for fraud or corruption activities.

There are several attempts on managing land information among them a researcher conducted a research which focus on developing a central database system using PostgreSQL software to retrieve, update and store the required data for urban land information management based on client-server architecture approach. [43]

Many of existing security solutions relies on a single trusted authority to verify information or store encrypted data in a centralized way. This leaves the system vulnerable to be accessed by unauthorized users and make control of and manipulate the stored records. Many bad actors could focus their efforts on a single target to commit the threats.

The security problems on records stored in the existing system in the agency as it's discussed in the above section which is mainly occurred due to improper manipulation of records and weak security mechanism used in the system which must be addressed by

creating a more secure environment which enable every stored records kept secured through and can protect the records against any adversarial to achieve the mentioned agency objectives.

This thesis therefore, aims at exploring the potential of blockchain technology in addressing the existing security treats of land record management.

1.3. Research Questions

The study focuses on the following research questions to achieve the objectives.

1. What are the current security challenges being faced by the Agency in managing digitized land records?
2. How can blockchain technology best serve in addressing the existing security challenges?

1.4. Objectives of the study

1.4.1. General objective

To ensure the security of the Digitized Land Records using Blockchain Technology in Addis Ababa City Administration Land Holding Registration and Information Agency.

1.4.2. Specific objectives

In order to achieve the above general objective, the following specific objectives (activities) will be accomplished

- Studying the existing systems applied in the agency to manage land record.
- Identify existing security challenges of the existing information system.
- Review and study the works done so far in the area.
- Explore the potential of blockchain technology in addressing the existing security challenges.
- Develop a prototype for demonstrating the potential of blockchain technology in creating secured environment for digitized land records.
- Validate the prototype
- Forward recommendation on the implementation of blockchain technology and potential areas for future works.

1.5. Methodology

To achieve the main goals of this thesis these methodologies will be applied

- Extensive literature review will be conducted to get a deeper understanding the blockchain technology.
- Qualitative approach will be used for the data collection by using questionnaires, interview and on site observation for investigating the theories and practice of the implemented archive system in the agency from the headquarter office up to the selected sub cities.
- Design science approach will be used to develop a prototype using the appropriate blockchain technology.

1.6. Scope of the study

The scope of this study is limited to explore and demonstrate the potential of the blockchain especially Ethereum on preserving digital land record for Addis Ababa city administration land holding registration and information agency.

1.7. Significance of the study

Every single service in the agency is provided based on the owners record with correspondence with the respective manuals and procedures followed in the authorities. And each employee make decision and deliver service on the available records of a parcel so these records must be kept in a secure way where employees can use it on every activity of their service delivery. Using the blockchain technology in the land administration authority asserts the tamper proofing of records which manly have these significance.

- Provide a better security mechanism for land registration actors with more transparency
- Build trust on employees on the integrity of the data they are using while providing service and on their decision making
- Enhance the speed and efficiency of service delivery
- It can be inherited and adopted by other organizations facing the same problem.
- Deliver additional perspectives in regard to the current state of the technology and inspire researchers for further advancement in the area.
- Step the agency one step ahead to complete its digital experience.

1.8. Limitation of the study

The technology is a novel one with great features but these points might hinder the full realization and deployment of the technology

- Available equipment and infrastructure to build out the necessary network for the participants as of the requirements of the technology
- Scalability
- Lack of availability of data and records to be used due to the pandemic.
- Insufficiency of time and budget

1.9. Organization of the paper

This thesis paper is organized in to five chapters composed of different topics as outlined below.

Chapter-1: Introduction: - Provides background of the study, defines the research problem and sets out objectives of the study. It is also composed of a set of research questions to be answered from the findings and the significance of the study. The chapter also discusses the scope and limitations of the study. Finally, the organization of the paper planned to accomplish the objective is outlined in this chapter.

Chapter-2: Literature Review: - Gives basic concepts related with blockchain and record management and some related works will be discussed.

Chapter-3: This chapter defines the Research techniques and methodologies to be used.

Chapter-4: Discuss the analysis and design of the prototype.

Chapter-5: Implementation and evaluation of the prototype.

Chapter-6: Conclusion and presents recommendation for future work in the aspect of the possible future.

CHAPTER TWO

2. LITERATURE REVIEW AND RELATED WORKS

2.1. Introduction

Government agencies in developing countries are exploring ways to digitize land records to reduce the vulnerability of single-copy paper-based titles, and increase the reliability, authenticity and transparency of the land registration system. The involvement of multiple stakeholders, such as parcel owners, government agencies, and financial institutions made land registration a complex process. At the core, all the parties need to trust the system that keeps track of land ownership, and the legality of the titles registered therein. While property information varies by country and jurisdiction, and it is regulated by specific legal frameworks, the goal is the same to provide a system for recording titles of ownership and facilitating the legal transference of land property rights. [2, 3, 4]

In blockchain technology, the transactions can be registered without the services of any trusted third party. It is a method of recording data - digital ledger of transactions, agreements, contracts anything that needs to be independently recorded and verified. It knows who owns what at a certain time. It keeps track of transactions, it knows when a transaction took place and it ensures that there is always one single owner of any item or unit and no double usage is happening of the same. [11]

This section will try to review and present a brief overview of the blockchain technology and main components also its utilization on the record preservation.

2.1.1. What is blockchain?

A blockchain is a distributed tamper proof public database which stores its transaction data in containers called “blocks”. Each created block is linked to the parent block through digital fingerprints called “hashes.” These hashes are publically time stamped in a header at the top of each block of information. This history of transactions stored on the blocks can be linked back to the initial or “genesis” block. The information stored in blocks is resilient against tampering and corruption even by those who store and process the information. This is made possible by independent nodes that come to a decentralized consensus for all transactions

which have occurred. [48]

Blockchain is a decentralized distributed database of records storing hash values of data, information, transactions, documents or records and it is associated with the concept of distributed ledger technology (DLT). The name is composed of two terms “block”, which refers to the complete set of contents, and “chain”, which refers to the interconnection of the blocks. [23]

It's a distributed digital ledger in which the cryptographically signed transactions are grouped into blocks. Each block is cryptographically linked to the previous one after a validation process and undergoing a consensus. As new blocks are added, older blocks become more difficult to modify which makes blockchain tamper resistant. New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules. Blockchain is implemented through a peer-to-peer network in which each connected computer (node) stores data on all. [11]

Blockchain is mainly characterized by high tamper-resistance, which has lack of defined central operator that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network. Besides allowing cryptocurrencies to be transferred, blockchain allows for a variety of types of digital information or data (digital assets) to be shared or distributed. A blockchain maintains a continuously growing list of transactions or uploaded digital data, time-stamped with the hash of the previous block connecting to the next block to preserve the chain integrity. [16]

The underlying technologies and concepts of the blockchain and distributed ledger technologies are based on these concepts. Those are hash algorithms, Merkle tree, distributed consensus. [17, 23]

2.1.1.1 Hash algorithms

Hash, or message digest, is a one-way function that quickly calculates a unique fixed-length string out of any data, information, document or record of any size. The one-way characteristic means that it is not possible to recreate the original document by knowing its hash. It is extremely difficult and nearly impossible to create “collisions”, which makes

unable to have two or more meaningful records with the same hash value. The resulting hash value is also referred to as a digital fingerprint. [18, 22, 27]

2.1.1.2 Merkle tree

Hash values may be grouped together to form one hash. Based on the number of documents created a hash value is calculated for each document. At every hour, all hash values from all documents are grouped and hashed together to get just one “hourly” hash. At the end of the eight-hour working day, all eight “hourly” hash values are hashed together to get one hash value for a day. This hash is called root hash or top hash. The approach was first introduced by Ralph C. Merkle in 1980 and the structure resembles a tree (upside-down), it was named as the Merkle tree. [18, 22, 27]

2.1.1.3 Distributed consensus

Blockchain uses a distributed (peer-to-peer) network in which all interconnected computers are treated equally. This type of network has no single point of control and therefore no single point of attack. Blockchain uses the principle of distributed consensus in which every participant (node) records every event in their ledger. Consensus is used in order to ensure that all ledgers are exact copies and to determine the truth. The event is valid only if the qualified majority of the nodes that is (50%+1 node) agree. [18, 22, 27]

2.1.2. Essential Characteristics Related with Blockchain

Time-stamping:- every entry created in the blockchain is securely tracked with a time-stamp which makes backlogging impossible. [18, 22, 27]

Accessibility:- all participants may have access to view the data on the chain or to add data depending on granted permissions. [18, 22, 27]

Smart Contracts:- a program coding of an electronic agreement, it defines the conditions to which all parties have agreed. When agreed upon conditions are met certain actions are executed. On every transaction a result of executing a smart contract can be verified by any other node by executing the same smart contract with the same inputs. [18, 22, 27]

Decentralization:- brings the distribution of power among the nodes where there is no single node that has authority over the network and each node will be sharing the same data

as the other. This distributed replica of the same set of chained blocks over the network brings the blockchain to be called a distributed ledger. [18, 22, 27]

Immutability:- it mainly refers to the transaction data and once data is entered it can't be tampered. The cryptographic hash linking of the blocks makes sure of the immutability. [18, 22, 27]

Ledger:- the technology uses an append only ledger to provide full transactional history. [18, 22, 27]

Secure:- blockchains are cryptographically secure, ensuring that the data contained within the ledger has not been tampered. [18, 22, 27]

Distributed:- the blockchain can be distributed.. This allows for scaling the number of nodes of a blockchain network to make it more resilient to attacks by bad actors. By increasing the number of nodes, the ability for a bad actor to impact the consensus protocol used by the blockchain is reduced.[18, 22, 27]

Shared:- the ledger is shared amongst multiple participants and this provides transparency across the node in the blockchain network. [18, 22, 27]

In general features of the blockchain can be formalized into a list of four core characteristics:

- **Immutable** (permanent and tamper-proof) a blockchain is a permanent record of transactions. Once a block is added, it cannot be altered which create trust in the transaction record.
- **Decentralized** (networked copies) a blockchain is stored in a file that can be accessed and copied by any node on the network which creates decentralization.
- **Consensus Driven** (trust verification) each block on the blockchain is verified independently via a consensus models which provide rules for validating a block, and often use a scarce resource to show proof that adequate effort was made. This mechanism works without the use of a central authority or an explicit trust-granting agent.
- **Transparent** (full transaction history) since the blockchain is an open file any party can access it and audit transactions. This creates provenance under which asset

lifetimes can be tracked.[11,27,37]

A small change in the data drastically changes the value of its hash where the newly computed hash has to be matched with the already linked chain of hashes. Also, the property of decentralization makes a very important role here because if a corrupted node tries to modify the data on its local state this has to be accepted during the consensus mechanism by all the other nodes which makes it difficult to modify the data. As a result it's called a novel kind of distributed ledger technology that uses cryptography to protect records during creation and storage which gives strength to crypto currency but it can also be used for other purposes as well. Many authors predict widespread use of this technology beyond crypto currencies including financial transactions, recordkeeping etc [16, 17, 18, 26]

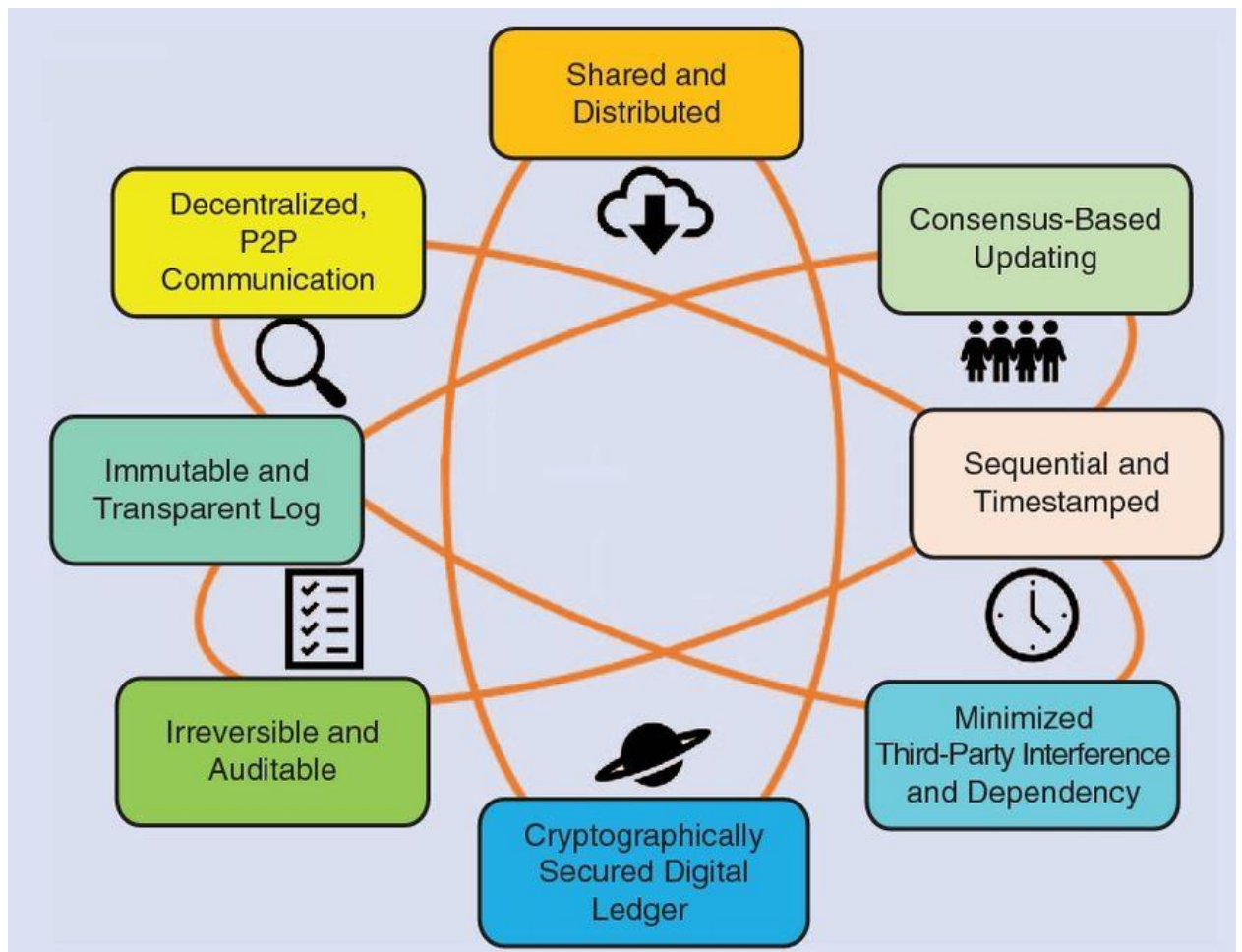


Fig. 2-1 vital blockchain characteristics (source [27])

2.1.3. Core Components of Blockchain and how they work

The blockchain setup and network operations are built upon these core components [24, 27, 29]

Node:- user or computer within the blockchain which install and run a computer application specific to the ecosystem they wish to participate in. Once one has a node application it can participate in the respective blockchain ecosystem.

Block:- a data structure used for keeping a set of transactions which is distributed to all nodes in the network and each block contains a block header and block data. The first block of a blockchain network that records the initial state of the system is called Genesis block.

Block data:- The portion of a block that contains a set of validated transactions and ledger events.

Block header:- The portion of a block that contains information about the block itself (block metadata), typically including a timestamp, a hash representation of the block data, the hash of the previous block's header, and a cryptographic nonce (if needed).

Chain:- a sequence of blocks in a specific order which is a linked list of hash pointers from the genesis block to the last block. The chain determines the chronological order of all transactions, as well as the integrity of the entire blockchain. One can verify the integrity of the chain by computing the hashes from the genesis block to the last one; if any hash pointer to the previous block differs from the one computed, the chain has been altered.

Miners:- specific nodes which perform the block verification process and the act of solving a puzzle within a proof of work consensus model are called Mining.

Shared Ledger:- It is a data structure managed inside the node application. Once you have the node application running, you can view the respective ledger (or blockchain) contents for that ecosystem. Regardless of how many ecosystems you are a participant in, you will only have one shared ledger for each ecosystem.

Transaction:- smallest building block of a blockchain system which is a recording of an event, such as the transfer of assets (digital currency, units of inventory, etc.) between parties, or the creation of new assets. The Blockchain enables the sharing and exchange of

information among nodes on a peer-to-peer basis. This exchange takes place by means of files containing transfer information from one node to the other, generated by a source node and broadcasted to the entire network for validation. The current state of blockchain is represented by these transactions, which are continuously generated by the nodes, and then congregated in blocks. On each generated transactions it is very important to validate and verify the genuine ones and discard the fake.

Virtual Machine:- The virtual machine is the final logical component implemented as part of the node application that every participant in the ecosystem runs. E.g Ethereum is a blockchain ecosystem, the virtual machine lives in the Ethereum node application, called a wallet and it can understand a wider range of instructions making it possible to manage the state of a digital contracts also known as smart contracts. The instructions take the form of a special programming language that instructs the Ethereum virtual machine in the node application to enforce the terms of the contract consuming and releasing a digital token called “ether” as part of the transaction. The contract cannot be tampered with, again because of the cryptographic integrity of information on the Ethereum blockchain. [24, 27, 29]

Asymmetric key Cryptography:- The blockchain network utilizes the capabilities of public key cryptography for secure operation of the blockchain. To perform any exchange, other than being on the same platform, the users need to possess a digital wallet (functioning like a bank account) secured with the user’s private key, and accessible with appropriate signatures generated using that private key. This wallet’s public key serves as the address known to everyone, which is advised to change with each transaction for maintaining privacy and anonymity of users where as private keys are used to digitally sign transactions and are kept secret by the user. [24, 27, 29]

Consensus:- logical component which have a set of rules and arrangements to carry out blockchain operations. It provides the ‘rules of the game’ for how the ecosystem will arrive at a single view of the ledger. Different ecosystems have different methods for attaining consensus depending on the desired features the ecosystem requirements. [24, 27, 29]

The algorithms run by the nodes of the network to agree on the state of the blockchain. The set of all transactions, in turn, defines this state when a new transaction is added, the state changes. Because of possible delays transmitting the new transaction to all nodes, the order

in which transactions arrive at a node may differ with respect to other nodes. Since there is no central authority node to decide which transaction arrived before, the consensus algorithm is run by the network and can be verified by any node, shifting the trust from a traditional central authority to a distributed verification through cryptographic methods. [24, 27, 29]

Consensus Mechanism:- When nodes begin data sharing and exchanging via a blockchain platform, they don't have a centralized party to regulate and resolve disputes or safeguard against security violations and a mechanism to keep track of the flow of shared and exchanged data to ensure an unassailable exchange to avoid fraud. [24, 27, 29]

All nodes should agree on a common content updating protocol for this ledger, to maintain a consistent state and blocks should not simply be accepted to be a part of the blockchain, without majority consent. This is called a consensus mechanism, by which blocks are created and added to the existing ledger for future use. This consensus is an agreement amongst the nodes, which involves block mining, where in miners compete to find the next valid block by computing a cryptographic block hash. This hash value is called 'the proof of work' and if all transactions and proof-of-work are valid, the nodes accept it by updating their copy. [24, 27, 29]

Consensus Algorithms

How to reach a consensus in blockchain environment is a challenge in order to reach an agreement over the next valid block of transactions, a consensus algorithm is used. Some common consensus algorithms are:

- **Proof-of-Work (PoW):** This algorithm is first used in Bitcoin and employs a node's Central Processing Unit (CPU) power to compete with other nodes in solving a hashing puzzle to retrieve a predetermined value [36,39]. Succeeding in doing this reward the node with consensus power, which is determined by a certain amount of newly gained cryptocurrency. Participating nodes, or miners, can do this alone or team up with other nodes. However, due to the amount of computational power required to succeed, PoW can be computationally expensive and high energy consuming. [47]
- **Proof-of-Stake (PoS):** The difficulty of the hashing problems solved to calculate a predetermined value is based on the assets owned by the node [15,17, 19]. Miners

with more assets will be more likely to create new blocks to add to the chain. This consensus method uses less computational power than PoW but may be unfair because nodes with more assets will dominate more. This may motivate poorer nodes to attempt to attack the network. [47].

- **Practical Byzantine Fault Tolerance (PBFT)**: This type of consensus algorithm involves settling disputes between nodes in a network, typically in consortium blockchains. The main goal of PBFT is to solve the Byzantine Generals Problem, where it is possible that some nodes in a network may be corrupt and attempt to send the wrong message. There is the assumption that no more than 1/3 of the total number of nodes in the network is faulty. The node selected for the transaction needs to receive a vote from 2/3 of the other nodes before being able to continue with the transaction and add a block to the chain [41, 44].
- **Proof of X (PoX)** consensus algorithms generally depends on a qualification to decide which node has the ability to generate a new block to add to the chain [45]. PoX algorithms are found to be used for public blockchains, where nodes are required to prove that they own a defined type of resource in order to participate in blockchain activities. However, blockchains that use PoX are at risk of malicious users creating fake nodes on the network in order to claim consensus power. Usually, in this case, the longest chains in the network are considered to be the trusted chain. However, this does not prevent unfair power due to some nodes lacking the resources required to partake in blockchain decisions. Consensus algorithms that are Byzantine Fault Tolerant avoid this by having a pseudo-randomly selected leader determine if a decision should be made according to the decisions made by each node. [45, 46, 47]

2.1.4. Block formation Phases of Operation

The complete block formation process in the blockchain can be put into two phases [24, 29, 30]

- 1) Transaction generation and verification
- 2) Consensus execution and block validation

1) Transaction generation and verification

A. Contents

Nodes or users connected within the same network have knowledge of each other's address before they begin any transfer. Transactions are uniquely identified by their transaction ID, which is the SHA-256 hash value of the input transaction and public key of the recipient. This is further encrypted with the sender's private key, for generating digital signatures to assist recipients in uniquely identifying the source. If any content is changed, it would consequently affect the Transaction ID as well as the signatures and in case of mismatch the transaction is discarded.

B. Confirmation of transaction

Every transaction will be confirmed with its existence in a valid block of the ledger until the time the transactions are confirmed, they are not considered trustworthy. Transactions are committed only if, upon reception of the transaction, and could verify the following:

- I.** The referenced input's transaction's unused transaction outputs (UTXO) is valid
- II.** Since only the user authorized to access the UTXO can use it in a subsequent transaction, the recipient checks for the valid signature which should match the UTXO owner signature.
- III.** The referenced transaction must be published in a valid block where existence of a transaction in a block confirms its validation.
- IV.** Conservation of value is a must, it is most important in checking a transaction's validity.

C. Claiming ownership

Every transaction produces an output redeemable by the recipient nodes authorized in the public key hash of the transaction. This public key hash authenticates users by uniquely identifying them in the network while preserving their privacy. Only those users who can generate valid signatures with their private keys can claim ownership for redeeming transaction outputs. [24, 29, 30]

2. Consensus execution and Block validation

Nodes, in the absence of a trusted party follow a consensus on how to confirm or discard blocks and transactions with mutual effort so that there aren't any conflicts at a later stage. A

cryptographic puzzle is to be solved for acceptance of any block and its addition in the shared ledger. This works by nodes accumulating the verified transactions in a block and putting their resources to find a value that makes the SHA-256 hash value of this block less than a dynamically varying target value. The block contents include the arbitrary nonce, hash of the previous block, Merkle root hash of the listed transactions, timestamp and block version. The term ‘proof-of-work’ refers to this random value which is found by the miners, by repeatedly hashing the block contents with many such random values to achieve the Cryptographic block hash. The necessary steps for block validation are:

1. All the transactions contained in the current block are verified by claiming ownership. After individual verification, the transactions’ chronological order conforming to their occurrences and references is confirmed.
2. The previous block’s hash referenced by the current block exists and is valid. This is usually checked from the genesis block.
3. Accuracy of time stamp is verified.
4. The proof-of-work for the current block is valid.

Block Header			
Block Hash	Tree Root hash	Time Stamp	Nonce
Previous Block Hash		Other Metadata	
Block Data			
Transaction Counter		Total Block Value	Total Block TX Free
Transaction(TX1)	Transaction (TX2)	Transaction (TX3)	Transaction (TXn)
Sender Address	Sender Address	Sender Address	Sender Address
Value	Value	Value	Value
TX1 Fee	TX2 Fee	TX3 Fee	TXn Fee
Receiver Address	Receiver Address	Receiver Address	Receiver Address

Fig. 2-2 Sample Block Structure (Source [26])

Description of elements in the block structure:-

Tree Root hash :- A Merkle root is the hash of all the hashes of all the transactions that are part of a block in a blockchain network. [27,41]

Block hash:-The primary identifier of a block is its cryptographic hash, a digital fingerprint, made by hashing the block header twice through the SHA256 algorithm. [27,41]

Time Stamp:-A timestamp is used as the proof of integrity that define the standard of certain documents or files that exists for a certain time period without relying on any third party authentication and also avoiding long term maintenance cost or needs. [27,41]

Nonce:-A nonce is an abbreviation for "number only used once," which is a number added to a hashed or encrypted block in a blockchain that, when rehashed, meets the difficulty level restrictions. Once the perfect Nonce is found, it is added to the hashed block. Along with this number, the hash value of that block will get rehashed and creates a difficult algorithm. [27,41]

Previous Block Hash:-Storing the hash of the previous block in the current block assures the integrity of the transactions in the previous block. Any modifications to the transaction(s) within a block causes the hash in the next block to be invalidated, and it also affects the subsequent blocks in the blockchain. [27, 41]

Sender /receiver Address:-This are the address the transactions take place among parties as a more general explanation, an Ethereum address (or wallet) is simply a 64 character hex string generated subject to various rules defined in the Ethereum. [27, 41]

2.1.5. Block acceptance and chain update

On the process of block acceptance and chain update by the nodes these two scenarios can occur:

- 1.** If the transactions contained in it are valid and the computed proof-of-work is correct nodes will accept the block. Nodes show their approval and acceptance, by adding the block to their copy of the ledger and advancing to find the next valid block, with this block as a predecessor, and taking its hash as the previous hash for the successive block. If two miners find a valid solution at the same time, only the longest blockchain is considered as valid where it made the blockchain a tamper-proof and once changes are made it cannot be reversed. [24, 29, 30]
- 2.** If the transaction in the block or proof-of-work is not valid, the block will be discarded

and nodes continue to find a valid block.

Among the several strengths in the blockchain concept the mains points are only hashes are stored (registered) in the blockchain. The actual data, documents or records being hashed are stored in the institutional document or records management systems. Also each additional block reinforces the preceding ones, since the blocks are chained together and each new block is dependent on the links of the previous blocks. Finally, modifying any block on the chain invalidates all subsequent blocks. [24, 29, 30]

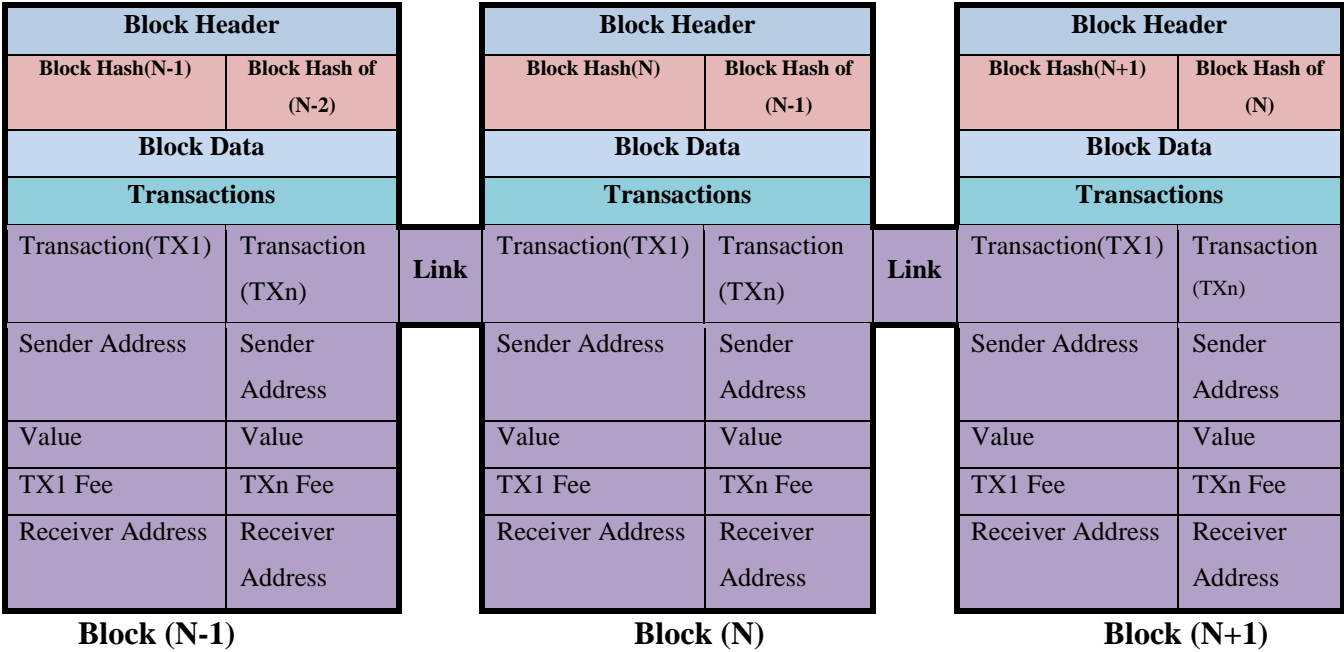


Fig.2-3 Sample blocks in blockchain (source [26])

2.1.6. Blockchain Types

Based on the nature of data accessibility Blockchain can be categorized as Public, Private, Community/Consortium and Hybrid Blockchain. ,

1. Public Blockchain

It is a type of blockchain, where anyone can read and submit transactions in which there are no restrictions on data reading or sending of transactions in the blockchain.

For example, in Bitcoin and Ethereum, there is no centralized party or group of parties that is said to own or control the network. As a result, core developers actually wield a great

amount of control, even though individual nodes may be free to join or leave a blockchain. [22, 23, 25, 26]

Main properties of public blockchain are:-

- Designed to be fully decentralized, with no one individual or entity controlling which transactions are recorded in the blockchain or the order in which they are processed.
- Highly censorship-resistant, since anyone is open to join the network, regardless of location, nationality, etc.
- All have a token associated with them that is typically designed to incentivize and reward participants in the network. [22, 23, 25, 26]

2. Private Blockchain

In this type of blockchain only one organization or all subsidiary organization within same group are allowed to read and submit transactions in which direct access to data and transactions sending is limited to a certain narrow range of participants. [22, 23, 25, 26]

All of the technical components of the blockchain are owned and operated by limited participants. Such blockchains are generally less trusted because it is technically possible for an entity that owns and operates the entire infrastructure to manipulate its operation in order to alter the ledger, though in practice there may be many socially-defined incentives like laws, investor disapproval that would prevent this from happening. [22, 23, 25, 26]

Mainly Private Blockchains are valuable for enterprises that want to collaborate and share data, but don't want their sensitive business data visible on a public blockchain. These chains, by their nature, are more centralized; the entities running the chain have significant control over participants and governance structures. [22, 23, 25, 26]

Main properties of Private Blockchain are:-

- Participants need consent to join the networks
- Transactions are private and are only available to ecosystem participants that have been given permission to join the network
- More centralized than public blockchains
- May or may not have a token involved with the chain [22, 23, 25, 26]

3. Community/Consortium Blockchain

It is sometimes considered as a separate designation from private blockchains. The main difference between them is that consortium blockchains are governed by a group rather than

a single entity. This approach has all the same benefits of a private blockchain and could be considered a sub-category of private blockchains, as opposed to a separate type of chain. In this type of blockchain multiple group of organizations form a consortium and are allowed to submit transactions and read transactional data. [22, 23, 25, 26]

4. Hybrid Blockchain

This is a new category where any of three Public, Private or Community/Consortium, blockchain can be combined to facilitate transactions. A blockchain platform can be configured in multi-mode using Hybrid Blockchain. [22, 23, 25, 26]

Platforms combine the privacy benefits of a permissioned and private blockchain with the security and transparency benefits of a public blockchain. That gives businesses significant flexibility to choose what data they want to make public and transparent and what data they want to keep private. [22, 23, 25, 26]

Based on the need of authorization to participate in Blockchain it can be categorized as Permissionless (inclusive) Permissioned (exclusive) and Hybrid Blockchain.

1. Permissionless (inclusive) Blockchain

No prior permission is needed to participate in this type of blockchain. Everyone allowed to participate in verification process and can join blockchain network with their own computational power. Participants do not require special authentication or authorization to access, read, write and participate in transactions and in the consensus process. Examples of permissionless blockchains are Bitcoin and Ethereum. [22, 23, 25, 26]

2. Permissioned (exclusive) Blockchain

Only authorized parties are allowed to join this type of blockchain and run nodes to verify transactions in blockchain network.

The processing of transactions is carried out by a certain list of identified persons and nodes must have a member identity and participants must authenticate (e.g., enter a user name and password) to gain access and must have authorization to use the system resources. Permissioned blockchains have membership services that manage the identity, privacy, confidentiality and auditability within the system. [22, 23, 25, 26]

3. Hybrid Blockchain

This provides the possibility that a node is participating in Permissionless and Permissioned Blockchain together to facilitate inter-blockchain communication also configured to support Permissioned and/or Permissionless model. [22, 23, 25, 26]

Based on the core functionality and smart contract support in concern, Blockchain can be categorized into Stateless and Stateful Blockchain.

1. Stateless Blockchain

These systems only focus on transaction optimization and chain functionality that is verifying the transaction by computing hashes. It is independent from smart contract logic layer thus unaffected from smart contract code bugs and vulnerabilities. [22, 23, 25, 26]

2. Stateful Blockchain

This type of blockchain provides smart contract and transaction computing capabilities. It also supports multifaceted business logic, its optimization and preserves logic states. [22, 23, 25, 26]

2.1.7. A brief history of Blockchain

Even if Bitcoin Satoshi Nakamoto is approved as a founding figure of blockchain many experts declares that the history of blockchain stretches back further than Nakamoto's 2008. Here are some researchers and their contribution that can be mentioned in the history of blockchain. [15, 20, 21, 37, 38]

David Chaum: Blind signatures and e-cash (1982)

In 1982, David Chaum proposed a scheme that used blind signatures to build untraceable digital currency. In this scheme, a bank would issue digital money by signing a blind and random serial number presented to it by the user and the user could then use the digital token signed by the bank as currency. The limitation to this scheme was that the bank had to keep track of all the serial numbers used for this purpose. This was a central system by design and required the trust of the users.

Adam Back: Hashcash (1997)

The Hashcash, was originally introduced in 1997, to prevent unwanted, or spam email. The main idea behind Hashcash was to solve a computational puzzle that was easy to verify but relatively tough to compute.

Wei Dai: B-money (1998)

The concept and idea of using a Proof of Work have been introduced and used to create money. A major weakness in the b-money system was that an adversary with higher computational power could generate unsolicited money without allowing the network to adjust to an appropriate difficulty level. This system lacked details on the consensus mechanism between nodes and some security issues, such as Sybil attacks, were also not addressed.

Nick Szabo: Bit gold (1998)

Despite being based on the Proof of Work mechanism, Bit gold had the same problems as b-money except that the network difficulty level was adjustable.

Tomas Sander and Ammon TaShama: e-cash (1999)

Introduce e-cash schemes which used Merkle Trees for the first time to represent coins and zero-knowledge proofs to prove the possession of coins. In the e-cash scheme, a central bank was required to keep a record of all used serial numbers. This scheme allowed users to be fully anonymous, although at a computational cost.

Hal Finney: Reusable Proof of Work - RPoW (2004)

It was introduced by Hal Finney in 2004 and used the hash cash scheme by Adam Back as a proof of computational resources spent to create the money. This was also a central system that kept a central database to keep track of all used Proof of Work tokens. Additionally this was an online system that used remote proof, made possible by a trusted computing platform which also referred to as Trusted Platform Module (TPM) hardware.

Satoshi Nakamoto: Bitcoin (2008)

Satoshi Nakamoto leveraged current network technology to implement a Peer-to-Peer (P2P)

system for exchanging virtual cash. All the peers on the network operate as equal actors participating through the same protocol and which is self-regulated by its open network of computers. Thus, through Bitcoin, the world witnessed the emergence of a new phase of money. [15, 21, 37, 38]

2.1.8. Evolution of Blockchain Generations

BLOCKCHAIN 1.0: Bitcoin and cryptocurrency

The emergence of Blockchain defined the state of the distributed ledger as virtual coin, known as Bitcoin Blockchain. This virtual currency allowed users to do financial transactions and is also called the Internet Cash. The currency is named as cryptocurrency as each coin defines an electronic signature where the private key is used for signing the transaction and public key is used for verification. [15, 20, 21]

The main important properties of Bitcoin (Blockchain 1.0) are

- Successfully resolved the double spending problem
- Decentralization of currency and financial transactions
- Consensus Mechanism (Proof of Work) to verify all the transactions and maintaining the same state of blockchain across all the nodes in a distributed system.

BLOCKCHAIN 2.0: Smart contracts and Ethereum

Beyond Bitcoin: Ethereum and Smart Contracts

Due to the limited capabilities of Bitcoin to suit the needs of a general purpose application a requirement of general purpose development platform was felt. In 2013, Ethereum [12] was introduced which addressed several limitations in Bitcoin Scripting which is built in Turing Complete programming language. Thus, it supports all type of transactions, including loops that provide a virtual abstraction and anyone can create their own instructions for ownership, the format of the transactions, and define the state transition function.

The launch of Ethereum blockchain not only gave the world a newer and better cryptocurrency in the form of "ether", it also gave the blockchain community a new perspective on using the blockchain technology by the introduction of developing "Decentralized Applications (DApps)" by utilizing the Smart Contracts. Ethereum thus

paved the way for Smart Contracts, which are small computer programs that live and execute on the blockchain. They work autonomously and execute automatically, based on specific predefined conditions for validation of a transaction. Thus smart contracts reduce the cost of verification, arbitration and fraud prevention and allow transparency. The smart contract code is stored, verified and executed on a blockchain where each transaction consists of nonce, ether balance, contract code hash, and storage root. [27,28]

BLOCKCHAIN 3.0: Convergence towards decentralized applications

As smart contracts are growing every day, the current technology cannot support such volume of transactions even though Ethereum improved the transaction rate to 15 transactions per second (tps) over bitcoin 7 tps, still it is not sufficient to support today's economy. Hence, Blockchain is currently shifting towards decentralized internet, which will integrate data storage, communication Networks, Smart Contracts and Open standards platforms thus; there is need of Decentralized Applications (DApp). DApp have their backend running on a blockchain Network and can have a frontend code and user interfacing in any programming language that can call the backend for functionality support. [15, 20, 21]

DApp have the following properties [32]:

- Open Source platforms for coding support,
- Internal Cryptocurrency Support,
- A token that quantifies all credits and transfer in transactions within the system, and
- Decentralized Consensus mechanisms

BLOCKCHAIN 4.0: Seamless Integration with industry 4.0.

The current specifications of Industry 4.0 require an enterprise resource planning platform which can provide automation and integration of different execution platforms as a single coherent unit. This demands for an increasing degree of trust and privacy, thus a scalable blockchain network is required. This is where Blockchain 4.0 fits, allowing the IT systems to do business integration, operating on Cross-Blockchain business processes like allowing for autonomously placing an order via smart contract as well as ensuring safety to machines. This will support Supply-Chain Managements, Financial management systems, Health and

IoT Workflow Management and asset management. Thus, in short Blockchain 4.0 is decentralizing Blockchain 3.0 to operate in real-life industry and business logics to satisfy the requirements of Industry 4.0. [15, 20, 21]

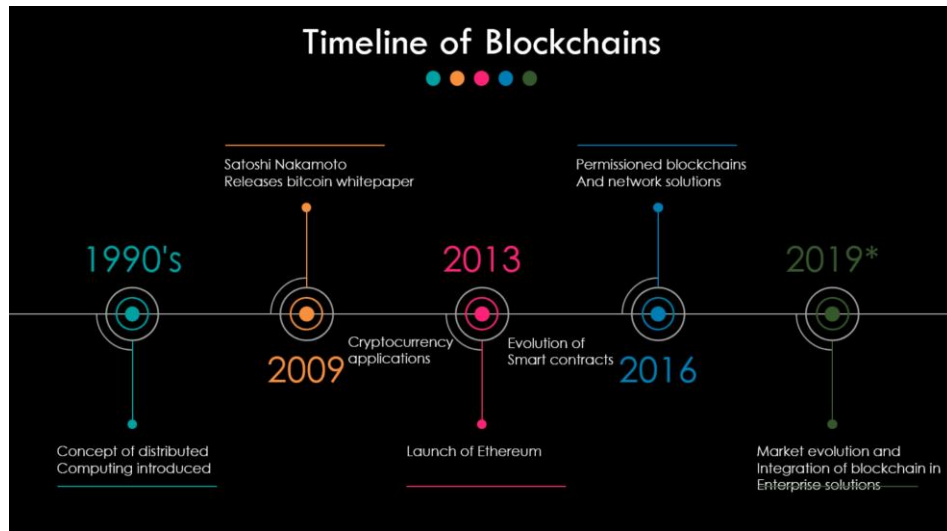


Fig.2- 4 Historical evolution of blockchains (source [15])

2.1.9. Records and Its preservation

Nowadays digital documents can be created in two ways – they can be digitized from existing paper records or be born digitally. The virtual nature of digital data along with the evolving hardware and software that surrounds it creates more challenging environment for preservation. It is important to note that every digitally preserved record should have its characteristics of authenticity, reliability, integrity and usability. To be successful, seemingly redundant practices need to be implemented. These practices should be periodically reviewed for their availability and effectiveness over the lifetime of the records' existence. Together, these practices create layers of insurance to safeguard the health and preservation of records. [5]

Mainly records preservation systems offers issues on those responsible for both public and private land records repositories and must develop an understanding and strategy for records preservation.. The goal should be to prevent the loss of even a single record. The on-going existence and authenticity of land records as captured require continuous attention for effective preservation and also laws and regulations, which set records management policies to change while new technology options advance rapidly. [22, 28]

Any effective records preservation program should include four vital components which are the ability: - [5]

1. To confirm the existence of a record at any time
2. To authenticate the record
3. To maintain file uniformity or track acceptable file formats, and
4. To recover the authentic record if it has been lost or corrupted.

One of the key steps in preserving any digital record is to identify the precise characteristics of the record, including all the objects or components that make up that record. It is necessary, therefore, to understand the significant technical properties of any digital object so that these properties can be preserved. [5, 13]

There are two overarching approaches to the preservation of digital records: passive preservation and active preservation. Passive preservation is the process of ensuring continuing integrity of and controlled access to digital objects along with their associated metadata. Essentially, passive preservation aims to ‘keep’ the original digital object intact without changing the technologies used to store or process it. [13, 28]

Active preservation seeks to ensure the continued accessibility of records over time by actively intervening in how records are stored and managed. Active preservation involves ‘moving’ the digital object into a new storage environment, which may depend on new technologies that were not in existence when the object was originally created and used.

Both passive and active preservation require that the integrity of the original digital object be protected. This integrity is protected either by preserving the original digital object just as it was when it was created, or by recreating the essence of the object using new and different technologies from those originally used.[13]

2.1.10. Blockchain and Land Record Preservation

Land Records are permanent records which include documents that retain legal, historical, and administrative value without any timeframe limitations. Responsibility for permanency rests on the shoulders of the current records custodians and their successors. [13]

The land registry office in all countries typically concerned on:

- Matters of ownership, possession or other rights of real property that are recorded and preserved;
- Maintaining records regarding land and other real estate to properly assess its value and to collect property taxes
- Developing internal confidence between its people, commercial enterprises and governments are manifested and promoted even if there are plenty of countries which does not have the trust of its people;
- The documents and data that are recorded the information that shows legal ownership and provides individual and enterprise protection.

Land registration systems record property rights and provide evidence in relation to property title holders. Regardless of a country's implemented land registration system, the primary aim of all such systems is to ensure title certainty. A non-transparent land registration systems, as well as inadequate land laws and enforcement procedures can have a negative effect on the whole registration system leading to a situation of title uncertainty. In addition, a land registration system which is centralized and paper-based could potentially lead to the loss of rights following a natural disaster. [9, 13, 15]

Also land registration systems record the relationship between the object i.e. the property, the right at law and the subject i.e. the right-holder who holds the property in question by way of ownership or any other right. This multilateral relationship is oftentimes complex in nature, in view of the different rights over the same object which may be held by different subjects and/or in multiple shares. On the other hand, there exist several limitations with land registration systems currently implemented by countries which affect land title certainty. Advancement in technology may aid with providing a more tamper-proof and secure registry which would ultimately lead to further protection over an individual's property rights. [15, 22, 23]

A step-forward from having a paper-based land registry is to actually digitize the system by digitizing land records, so that land registration systems would be reducing certain risks which are primarily attributed to paper-based systems, resulting in an increase in the registry's reliability and transparency. Nevertheless, digitized systems would remain

vulnerable to fraud, error or the alteration of records, thereby bringing into question the very integrity of the records. Thus, when implementing a blockchain land registration system or preservation of the records, this complex relationship must be factored in and the system must be adapted accordingly. [14, 15, 17, 22,]

Utilizing blockchain technology can help by eliminating the above mentioned risks, eventually providing us with trusted and reliable records of registered land titles. Blockchain is all about ownership over digital assets, whereby the owner's details can be stored within such systems to allow for more traceability in relation to the owner of the asset in question. [15, 31, 35]

Blockchain technology has many characteristics which may provide further certainty over the contents which are to be stored in the land registry. Having a complete record is a must, as otherwise doubts and uncertainties will always be present. Thus, it is of utmost importance that a country's legislation requires that anything affecting property rights be recorded within the registry. It is only after this is ensured that a blockchain-based land registration system would be able to provide us, with certainty, a true picture of what rights are held by a person (legal or natural) over a specific property. [31, 36]

As many governments, particularly in developing countries, continue to grapple with land governance and administration challenges, including the digitization of their registries, blockchain is still a long way from being implemented at scale. However, there may already be potential to pilot initiatives in smaller sub-areas where governments have been able to establish a strong record of land titles. Moreover, the advent of new advanced technologies such as satellite imagery, Geographical Positioning System (GPS), aerial imaging, and machine learning are increasingly offering new possibilities for digital land records to be completed at large-scale and low-cost in developing countries. These technologies will play a highly complementary role in establishing blockchain registries in the near future. [15, 31, 35]

Blockchain-based land registries system or preservation of the records will provide a vast improvement over today's paper-laden and sometimes cumbersome digital processes. Ultimately, it will support and strengthen land governance policies and systems worldwide. [31]

Emerging technology like blockchain features can be deployed to solve these problems related to the security of devices, networks and their users. Blockchain utilizes encryption and hashing to store immutable records and have the upper hand over current security measures which are decentralized.

The stored records are secured through the public key cryptography that protects against adversarial attempts to alteration of unauthorized access, whilst network users are assigned with private keys for validating and signing transactions. On every actions requests are sent to all the participant nodes and each check for the validity of the request if everything goes according to the business logic and transaction is valid all the ledgers will be updated and new block will be added. Records added to the ledgers are immutable and can easily be managed, audit, verify and increase the incredibility and transparency of the system.

Generally in the context of records management and its preservation and taking into account all characteristics of the blockchain as well as its underlying technologies and concepts, it could be concluded that the blockchain can be used to: confirm the integrity, existence or creation time of a record at certain point in the time and sequence of records in long-term preservation of records. [17]

2.1.11. Features of Blockchain technology in land record management

The critical feature of the blockchain that makes it today's most potential technologies are: decentralized, self-control, peer- to- peer relationship, fixed record and time stamping. It follows a method of passing data (such as records, events, or transactions) from one party to another in a very secure way. It is an electronic record of information that requires digital security all data stored in the blockchain is immutable; once a piece of data enters into a blockchain, it is practically impossible to alter its value. Blockchain in the land registry has been an essential aspect of today's world because once the land transfer task completes, the information automatically updates and saved on that blockchain platform, and this process is the safest and tamper-free mode of the operating system. No one can change the legal right of the ownership and can damage the data asset others cannot make a change in that transaction and ownership.[35, 46]

The use and implementation of Blockchain in the land registry and its assistance in maintaining the land records are quite transparent. Blockchain helps to make the process of

land registry transparent, straightforward and more accessible. It also empowers us to know if there had been any activities in a particular land. It shows every record of the land registered. This application will indeed take us towards development and easy accessibility to life not only for us but also for the future generation. Blockchains makes accelerate the process easier, fastest, and trustworthy to deal with businesses as it follows reducing fraud cases and bringing transparency with Smart contracts. [35, 46]

2.2. Related works

Blockchain is the most recent technology in the area in which scholars are conducting researches. Among these, the most relevant to our research are reviewed and presented in this section.

The authors [5] presented their work by exploring the process of digitalization of land records using blockchain technology focusing on two contrasting land-registry blockchain implementation initiatives: Honduras and Georgia. The research question that motivated the study was: Which factors affect the IS readiness of a public organization when adopting an emerging technology such as Blockchain? They have studied two pioneering initiatives of blockchain for land registry to understand how socio-political and technical issues influence the IS readiness of public organizations. Due to the experimental nature of the study they rely on an inductive approach by analyzing two case studies to extend Peled's (2001) theoretical framework (Eisenhardt 1989; Yin 2017).

They first conducted two unstructured interviews with the cooperation between Factom and the Honduran government to understand the challenge of land titling, map key stakeholders in the process, and that will help to understand the value and challenges of blockchain technology in land registry compared to existing methods. In addition to the interviews, they gathered secondary data from interviews and official sources to help them enrich the data and be able to present two similar initiatives of blockchain based land registry in two different countries Honduras and Georgia.

Totally any change in business processes in the public sector requires a combination of technology expertise, infrastructure readiness, and mechanisms for overcoming resistance. When the change involves the adoption of new technology, partnering with private firms

offers a vehicle to access technology expertise. The innovation can only succeed if the underlying records and infrastructure are ready for the transformation and if there is cooperation from all the parties involved, including mechanisms to neutralize resistance from embedded interests. All of these factors contribute to IS readiness with is a pre-condition to successfully move from coalition to institutionalization.

Finally, they introduce a theoretical framework that studies the politics of technological innovation in the public sector which can provide direction in future development and implementation of blockchain-related projects in the public-sector, particularly in developing countries. There is a need to identify the enabling and constraining factors related to the digitalization of public records and the adoption of land-registry blockchain initiatives. The underlying infrastructure and processes plays an important role in the feasibility of blockchain digitalization of land records. Regarding technology, every organization needs to assess the state of their IT infrastructure, and redesign processes especially for land registration, readiness factors include adequacy of business process and legal issues.

The authors [19] conducted a research on identified gaps which is a lack of authenticity and integrity of digital contents that are available online which are not tampered-proofed. Also they have focused to provide a framework solution which can be easily extendible, adoptable and used to provide the originality, authenticity, as well as integrity for any other digital records.

After reviewing different literature to brief the background on existing approaches they develop a system using solidity to write the code using the web browser-based IDE, Remix and smart contracts of Ethereum blockchain. The system uses smart contracts to trigger events that are logged to notify the participating parties to keep track of events and transaction details also implemented and verified the functionalities of the smart contract.

They proposed a solution that makes use of both blockchain smart contracts and Inter Planetary File System (IPFS) and a framework for providing authenticity of published online books and digital content. It provides decentralized storage and governance with different versions of the original book being stored, tracked, and traced with high integrity, and resiliency to all other forms of digital assets.

Their work has limitation on the deployment of the smart contracts on the real IPFS and they haven't used Ethereum network and develop frontend Decentralized Applications (DApps) with different views to different participants.

The author on [49] explores the usage of blockchain technology for land records management in the case of India. They have identified the existing land records available in the country are not clear, poorly administered and often, do not reflect the ground reality. Maintenance and availability of information of land records are a critical challenge faced by the government. This information is updated and stored by different departments at the district or village level. The data among these departments is not synchronized regularly, which creates differences in the records and often the information on the document's mismatches with the ground position. Poor handling of the processes of land transaction and record keeping affects the management of land markets in the country. They raised a research questions like how the Blockchain solution shall be used in the States and how to use the channels and design of smart contacts for better control of the system?

They have identified five participant nodes those are Bank (Mortgage/Loan, Buyer, Owner), Notaries/Court (Property Deeds/Disputes), Survey and Settlement Department, SRO Deed registration and Deed issue Tehsil Office (Validation/Updating of records). They have used the Hyperledger Composer to design a blockchain system which is an extensive, open development toolset and framework to make developing blockchain applications easier which offers a number of SDKs to support various programming languages Node.js and Java.

The designed system is with a focus on smart contracts and will capture and permanently record each transaction done either through sale of a property, inheritance, court orders and land acquisition. It tries to solve the existing problems by reducing the potential of forgery and disputes, as well as the costs and time involved, for any given transaction, paving way to implement conclusive land titling system with title guarantee in the country.

It's known that on increasing of population growth there will be increasing of records and transactions. Their work will face a security problem on managing and preserving a huge amount of records on the system which will create a big influence and load on the Blockchain system performance.

Summary

At this time, for the rest of the country, where physical records exist, an extensive conversion effort would be necessary to move existing land records to the blockchain by using two parallel processes one that prioritizes titles that are subject to change due to buy/sale transactions, and another that converts existing titles with no modifications.

As seen in the above works are limited at the framework and theoretical discussion level, the active future work is to implement such framework and then further explore its full potential and implement it in a real-world environment. These above solutions share the idea of peer-to-peer distributed file system, where the data is shredded, encrypted, and distributed to multiple nodes in the network to ensure their safety and availability which has a limitation on the deployment of the smart contracts on the real IPFS and they haven't used Ethereum network and develop frontend Decentralized Applications (DApps) with different views. These features are extremely important if blockchain-based applications equipped with off chain data storage solutions are deployed in operational and sensitive environments such as the financial and public sectors which will be tried to be filled by this study. Note that, the blockchain technology such as Ethereum is still at its early stages of development and therefore the future work would be the application of the appropriate version of blockchain technology in public sectors to meet and increase the security and privacy of individual's records.

CHAPTER THREE

3. RESEARCH METHODOLOGY

3.1 Introduction

Research methodology is the specific procedures or techniques used to identify, process, analyze information about a topic and way to systematically solve a problem. It could be understood as a science of studying how research is done scientifically and essentially, the procedures by which researchers go about their work of describing, explaining and predicting phenomena. Research methodology is a collective term for the structured process of conducting research. There are many different methodologies used in various types of research and the term is usually considered to include research design, data gathering and data analysis. Research methodology seeks to inform: Why a research study has been undertaken, how the research problem has been defined, in what way and why the hypothesis has been formulated, what data have been collected and what particular method has been adopted, why particular technique of analyzing data has been used and a host of similar other questions are usually answered when we talk of research methodology concerning a research problem or study. [50]

As described above, research methodology is one of the most imperative sections of the research chapter which enable to achieve the objectives of the study. In this chapter the research method used in this research, research process and sources of data, data collection tools will be elaborated.

3.2 Research Design

This research started with a literature review, which aims to understand the current art of knowledge, to learn previous findings and existing gaps, also to extract new ideas. Then data collection instruments were used to explore the existing problems. The collected data was analyzed to extract useful information and used as an input for the design of a prototype. [63]

3.3 Research Approach

Research approaches simply refers to a way of doing research that require reasoning which is a process of utilizing present knowledge for making predictions, outlining conclusions or

developing explanations.

This study used a mixed method research approach i.e. qualitative and design science. Qualitative research incorporates evolving questions and procedures, data is gathered in the participant setting and researcher interprets the meaning of data - the reasoning is occasionally inductive.[59] Also Design Science Research (DSR) is seen as the other side of research cycle that creates, evaluates information technology artifacts intended to solve problems identified in an organization .[51]

In this study a qualitative research approach adopted as an empirical view that seeks to explore the existing system and business process in the agency and the design science research approach will be used to solve the identified problem through artifact/prototype/development.

3.4 Qualitative Research Approach

The qualitative research approach is usually used for the investigation of social phenomena, or in other words, situations in which people are involved and different kinds of processes in which what we want to learn about environments, situations and processes. [53] It is non-numerical, descriptive, applies reasoning and uses words in the aim to get the meaning, feeling and describe the situation. This kind of method is used to assess knowledge's, attitudes, behaviors, and opinions of people depending on the topic of the research. [50]

On the other hand qualitative research is also concerned with qualitative phenomenon that is phenomena relating to or involving quality or kind which is designed to find out how people feel or what they think about a particular subject or institution. [50]

3.5 Research Context

In Ethiopia land administration system is under the control of the federal gov't where all land administration activities are carried out under the jurisdiction at state level and in their concerned state/city and their respective branch offices with the similar business process, manuals and directives. The Addis Ababa Land Holding Registration and Information Agency is one of the branches of the Federal Land Holding Offices that follows the same procedures with its each branch offices in the city the so called sub city/kifle ketema so it can be said that the population characteristic of the city is a homogenous one. On this base the researcher selected the head quarter office of Addis Ababa City Administration Land

Holding Registration and Information Agency (AALHRIA) and the sub city Kolfe Keranyo branch office has purposefully selected as a research site. The sub city Kolfe Keranyo is selected because the researcher is also member of the area and can make proper communication with the participant that enable the researcher easily get the information needed.

Regardless of the homogeneity of the population the data was collected from employees of the selected sub city and head quarter used as a research context for collecting data for analysis of the existing system and business process. The result is generalized to represent the current situation of the agency.

3.6 Source of Data

The source of data in the study is the subjects from which the data can be collected for the purpose of research. The data are information or facts used in discussing or deciding the answer of research question and help to gain sufficient data for the research.

Sources of data are primary and secondary sources. The primary data refers to the data originated by the researcher for the first time which are directly collected from the research participants using interview, observation and secondary data is already existing data which cover different sources like technical document, a website, articles, annual reports. In this research both primary and secondary data source were used. [58]

3.7 Data Collection Tools

Data collection is the process of gathering and measuring information on variables of interest, in an established systematic fashion that enables one to answer stated research questions, test hypotheses, and evaluate outcomes. The data collection component of research is common to all fields of study including physical and social sciences, humanities, business, etc. While methods vary by discipline, the emphasis on ensuring accurate and honest collection remains the same. [55]

In this research interview, observation and document analysis data collection tools were used to explore the existing business process and current system in the agency also to gather basic requirements to the proposed system.

3.7.1 Document Analysis

Document analysis is a systematic procedure for reviewing or evaluating documents both

printed and electronic material. Whereas document analysis has served mostly as a complement to other research methods, it has also been used as a stand-alone method. Documents contain text (words) and images that have been recorded without a researcher's intervention. [57]

The document analysis in this research covered procedures, directives, user manuals that provided the researcher deeper understanding about the agency also helps and plays an essential role in the preparation for the interview.

3.7.2 Interview

Interviews are something more than conversation. They involve a set of assumptions and understandings about the situation which are not normally associated with a casual conversation.

Interviews are particularly useful for getting the story behind a participant's experiences. The interviewer can pursue in-depth information around a topic. Interviews may be useful as follow-up to certain respondents to questionnaires, e.g., to further investigate their responses. Usually open-ended questions are asked during interviews. [50, 56]

There are three fundamental types of research interviews: structured, semi structured and unstructured. Structured interviews are essentially, verbally administered questionnaires, in which a list of predetermined questions is asked, with little or no variation and with no scope for follow-up questions to responses that warrant further elaboration. [56, 63]

Conversely, unstructured interviews do not reflect any preconceived theories or ideas and are performed with little or no organization. Such an interview may simply start with an opening question and will then progress based, primarily, upon the initial response. [56]

Semi-structured interviews consist of several key questions that help to define the areas to be explored, but also allows the interviewer or interviewee to diverge in order to pursue an idea or response in more detail. [56, 63]

In this research a face to face semi-structured interviews were selected. This interview approach has been selected because it encourages two-way communication, flexibility compared with the others approaches, allows for the discovery or elaboration of information that is important to participants. It provides an opportunity to understand the features of adopted systems in the agency and to know the users opinion on the existing system and

their recommendation to the feature.

The interview questions focused in the area of their experience, opinion on using the existing archive system and to what extent does the system support their work. It also tries to cover their treat while using the system and additional features to be included in the system.

The data was gathered from both employees and administrative staffs. The participants were selected using purposive or expert sampling which is designed to provide information as participants are those who have the required status, experience, or knowledge of interest to the researcher which is suitable to gain relevant information directly from the experts using the existing system.

The numbers of the participants are determined based on the agency team organization structure and the criteria used for the selection is their extent of involvement on using the existing archive system and their role on the services provided by the agency.

The participant of the interview and their job title is presented as follows:

Head Quarter

- System design and development team: - two system developers, one system administrator, one database administrator and one team leader.

Kolfe Keranyo sub city

- Information communication technology team - one system administrator, one database administrator and one team leader
- Documentation team - two archive encoders, three documentation officers and one team leader
- Adjudication team - three surveyors, three planners and one team leader
- Cadaster registration department - two GIS expert officers, two cartographers and one team leader
- Land holding right registration team - two GIS experts, two real property registrars and one team leader

Table 3.1 description of participants

No	Educational background	Gender	Status	Number of participants
1	Computer science	6 Males 2 Females	6 BSC 2MSC	8
2	Information technology	2 Males 4 Females	5-Diploma 1- BSC	6
3	GIS	4 Males	BSC	4
4	Law	2 Females 3 Males	BA	5
5	Civil engineering	3 Males	BSC	3
6	Land Administration	3 Males 1 Female	BA	4
7	Urban Managements	1 Male	MSC	1

3.7.3 Observation Technique

An observation is a data collection method to gather knowledge of the researched phenomenon through making observations of the phenomena, as and when it occurs which help to understand fully the complexities of many situations. Observation is a more natural way of gathering data by using systematic description of the events, behaviors, and artifacts of a social setting which provide an opportunity to document the actions, behavior, reactions and additional environmental characteristics in students' natural environment. [57, 61]

The researchers, adopting this technique, attempt to understand the actual phenomena happening on the truck. There exist various observation practices, and the researcher role as an observer may vary according to the research approach. In this research the researcher is observer and direct participant technique will be followed because it helps the researcher mainly to observe and also occasionally participate in the activities and to refer the situation by presenting physically and capturing the relevant phenomena and understand, examine the real scenario and daily activities in the agency.

3.7 Method of Data Analysis

In analyzing the data collected, the content analysis and descriptive analytical methods would be used. Hence information was collected through review of documents, interviews as well as observation data was analyzed within the outline of the study objectives. The data have been analyzed by using qualitative techniques in content analysis description as well as narration. Finally based on the findings relevant conclusions and recommendations would be drawn.

3.8. Research Validity and Reliability

3.8.1 Validity

Validity refers to the extent to which a test measures what it is supposed to measure and how truthful the research results. The validity can be tested by different approaches. The whole research is ensured by triangulating the data through observation, interview, questionnaire and secondary data.

3.8.2 Reliability

Reliability is concerned with the ability of an instrument to measure consistently and the extent to which results are consistent over time.

3.9 Design Science Research Approach

Design science research as a method of doing scientific researches has been defined in several ways. The design science as a paradigm has its root in engineering and science of the artifact, it's fundamentally on solving problem through creative innovations which define the ideas, practices, technical capabilities, and products in which analysis, design, implementation, and information system use can be effectively and efficiently reached. [51, 52]

It provides a solution to an important and relevant business problem and creates an innovative artifact in the form of a construct, a model, a method, or an instantiation that is clear, verifiable, new, and interesting research contribution. It also involves an iterative search for an effective solution to the problem. [51, 52]

A Component-based design used which focuses on the decomposition of the design into individual functional or logical components that represent well-defined communication

interfaces containing methods, events, and properties to ensure component reusability. It also defines the major components of the new system and how they relate to each other. Component-level design defines the data structures, algorithms, interface characteristics, and communication mechanisms allocated to each component for the system development. A complete set of software components is defined during architectural design.[65]

Even though there are many design science research procedures, the following design science research process model is adopted for this research. Figure 3.1 shows the steps of the research procedure and each step of the adopted procedures for this research is explained as follow: [54]

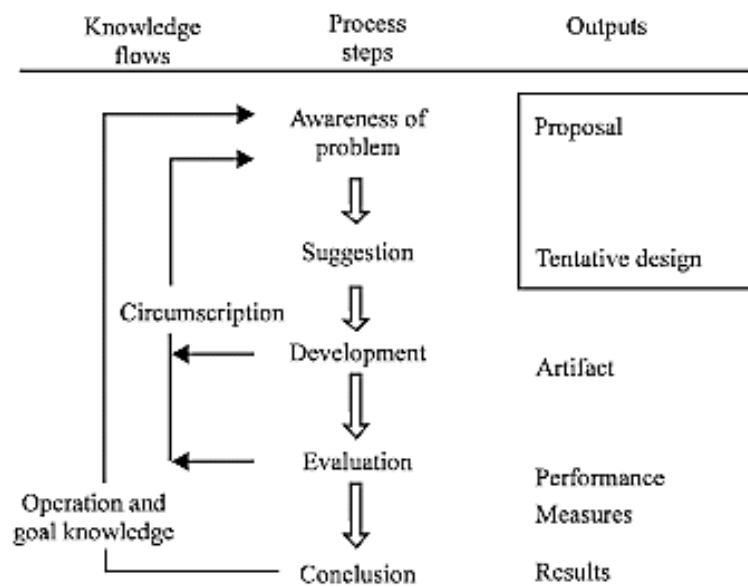


Fig. 3-1 General design cycle of DSR (Kuechler and Vaishnavi), source [54]

Awareness of a Problem

This first step of the adopted design science research methodology is awareness of a problem through problem identification and definition. This phase offers a solid and important foundation for the further research process. In this step, the researcher identifies the existing problem, understands different researches and studies in the area. [54]

The research proposal is the output of this phase in which the researcher is aware of the problem of a security threats on the integrity of the records and on preservation of records also attempts to show the opportunity of blockchain on addressing the problem. [54]

Suggestion

Following the development of a proposal based on the awareness of a problem the second phase is suggestion. This step is concerned with elaborated investigation of literatures on block chain and record preservation.

After problem identification, the researcher derives suggestions to address the identified research problem by reviewing more researches on block chain especially on record preservation system development. [54]

The researcher gathered detailed information which is relevant to fully understand the agency's procedures and requirements. This task delivers detail explanation to identify the business processes, drawbacks of the existing system and user requirements also features to be included within the domain area. Finally, the researcher analyzes the information and decomposes them in to activities. [54]

Development

The third step of the adopted research procedure is development in which the tentative design is further developed and implemented in this phase. In this step the working prototype will be developed as an output of the step. [54]

The researcher develops a web based record preservation prototype using:-

- Ethereum which is a software platform, used to build and deploy decentralized applications
- Ganache Personal Blockchain used to a local development blockchain and to simulate the behavior of a public blockchain.
- Truffle Framework which provides a suite of tools for developing Ethereum smart contacts with the Solidity programming language.
- Inter Planetary File System (IPFS) platform used to store and share files in a decentralized manner.
- ReactJs which is a JavaScript library used for building the user interfaces
- Metamask Ethereum Wallet which is a web browser which currently connect to blockchain networks.
- Solidity which is a contract oriented programming language used to write and manage the smart contracts.

Evaluation

Once the solution reaches a sufficient state it is evaluated according to criteria that are always implicit and frequently made explicit in the proposal. It is possible to iterate back to “design artifact” or even “identify problem” if necessary [54].

Evaluation can be achieved through the means of a case study or action research by arranging a broad expert survey (shows general interest) and laboratory experiments or simulations (used to compare different approaches). The researcher used human expert survey approach to evaluation of the prototype. [54]

Conclusion

This phase is the end of a research cycle of a specific research effort. The conclusion will show the significance and summary of the result achieved also suggestion to introduce a new possibility to explore different perspectives on addressing the issues of the research problem.[54]

CHAPTER FOUR

4. SYSTEM ANALYSIS AND DESIGN

Introduction

This chapter has mainly two sections, the first which is the system analysis part will describe and present basic points about the existing system based on the data collected using different methods and analysis model of the proposed system. Then after on system design section the proposed prototype main components and featured will be presented.

4.1 SYSTEM ANALYSIS

System analysis is a process of collecting and interpreting facts, identifying the problems, and decomposition of a system into its components. It is conducted for the purpose of studying a system or its parts in order to identify its objectives and also it is a technique of problem solving that improves the system and ensures that all the components of the system work efficiently to accomplish their purpose.

4.1.1 Overview of the existing System

Here the data collected through document analysis, observation and interview is presented to show how the existing system is developed, how it works and problems faced by the user while using the system.

The current system used in the agency which is called the archive system was developed with the objective to convert manual data handling system to computerized system which can address the problem of keeping records of archive files securely and provide paperless services for land owners. The system is a server based and developed using Microsoft SQL Server 2008 for the back end database and Microsoft Visual Studio 2010 C# to design the user interface and implementation.

a) Interview Results

Totally 31 respondents that are purposively selected from 6 teams with different profession and position have participated in the interview. Here is sample questions have raised for the

respondents for the end users and the one who participated in the development of the existing system accordingly.

- 1) What is your education level and in which field?
- 2) What is your Job Title?
- 3) How much is your land administration related Work Experience?
- 4) Have you had any experience on the archive system?
- 5) What security challenges are being faced?

Here is the overall opinions raised from the end users while conducting the interview

The system is a user friendly one which can easily be understood and accessible by the user. Even if it does not have all the features needed for delivering the service mainly it helps users to find or locate file on the lateral quickly and register, attach scanned image of the owner's record. The system helps to view the basic information of land owners whether or not it can get the requested service and then go back to the hard copy of the owner to cross check the completeness of data.

Integrity of records is the main issue here while delivering the services employees always check each of the hard copy of the customer record because there are times they found difference between what is registered in the system and the hard copies which is tampering of records is possible.. This gaps on integrity of records makes the service delivering a time consuming and to be dominated by the earlier manual system.

The system has to be changed in to a more secure one to protect the records in which that can prohibit the deletion of land owners record once it is stored so that anyone can use the system without any doubt and make decision, give services without checking the hard copies of the owners file that will make the service more faster and achieve the goal of the agency easily.

Here are the generalized opinions / answers gathered after conducting the interview from the experts who have participated in the development of the system

The encryption technique AED of length 64bit is used only for the user password. It is a server based in which the Data Base is managed by Head Quarter and only authorized

person login into the system. Any privileged user in the client machine can insert and delete the records. When the data is deleted by the end user it cannot be stopped/detected immediately but the system maintains history for all records in the log files and deletion can be traced from the log file later when there is an issues of suspect raised from the end users whose record is manipulated. Since land issues are very sensitive the manipulation of a single record can cause an immense crises and its consequence is very huge so a stronger encryption technique must be adopted to create a secure environment in the future.

When the system was designed one of the aim was to easily trace the location of the file from the lateral and this aim was achieved successfully. The rest and the main goal was to provide a paperless service for the customers using the system but this has not been achieved because of the potential threat of record manipulation by users which can open a way for deliberate fraud. So experts suggested that this problem of security on the integrity of records has to be addressed by developing a new tamper proof secure system and step forward the agency which will enable it to deliver a more trusted service in the future.

b) Data from Personal Observation

The researcher also proved through observation that the problems that respondents mentioned are still occurring and the effect is significant. The researcher also learned that there is a need to ratify the situation in the agency by introducing highly secured system.

The automated system had ease up the documentation and recording process by managing the files without redundancy and enabling easy to retrieval of files location on lateral. But the system didn't satisfy / answer issues raised by end users while using the system which prohibit them to use and back them to the manual one and which is improper handle the land ownership file recording system in a secure manner.

After observing, interviewing and document analysis in the agency business process the security problems in the current system is well known as presented in the above section. From the various technologies available in the area the researcher identified blockchain technology as solution to the identified problems by providing highly secured environment.

4.1.2 Proposed System

4.1.2.1 Overview of the System

Taking the drawbacks of the current Archive system into account, we have proposed a system for a secured record preservation that can store the tenure document basically by using the features of the blockchain technology. Since the technology of blockchain cannot store large files efficiently an Interplanetary File System (IPFS) is used to store and share large files more efficiently which relies on cryptographic hashes that can easily be stored on an Ethereum blockchain. Basically, the proposed prototype is based on Interplanetary File System (IPFS) and smart contracts of Ethereum blockchain where the record is accessed and shared on a tamper proof environment.

4.1.2.2 Requirement Analysis

Requirement is a feature that the system must have or a constraint that must be satisfied to be accepted by the client.

Functional Requirement

The functional requirement of the system is concerned with the functionality that the system should provide to users. This system is designed to register and preserve land records in a secure way.

The functional requirements are listed as follows:-

- Creating and managing accounts of the system users
- All authenticated users able to access the system.
- Be able to easily grant access permissions to users for records to be effectively shared and accessed.
- Registering records of owner parcel information and attaching the scanned images.
- Securely handling all the registered records.
- Granted users should access and view the registered records as requested.

Non-Functional Requirement

The non-functional requirement of the system deals with how well the system provides service to the user.

- The system will be designed in such a way that it can be maintained by the system developer or any authorized professional also should be flexible enough to accommodate the future needs of expansion.
- It should be easy to use and reasonably easy to setup.
- The system interface that will be in a web-based format can be accessed by nodes using acceptable browsers to access the blockchain.
- The system should always be available for the authorized user.
- The system should be secured to avoid unauthorized access and ensure the integrity of all the registered records.

4.1.3 Actors of the System

An actor describes any entity that interacts with the system. In this system, the interaction of actors with the system is through the web interface. In the proposed system, the following actors were identified.

Table 4-1 Actors of the system

Actors	Description
System Administrator	System administrator is a person who maintains and administers users and the system.
Right Registrar	A person in charge of making decision on papers to be attached in the systems which are basic/necessary for decision making while giving the service.
Archive Encoder	A person who will register records and attach scanned records of each parcel owners.
GIS Expert	A professional who will give service and make decision on spatial data to customers based on the registered record.

4.1.4 Use Case Diagram

A use case can be defined as a way in which a user interacts with a given system in order to achieve a goal. The figure below Fig. 4-1 shows the users' role in the designed system and how the system communicates with the end users.

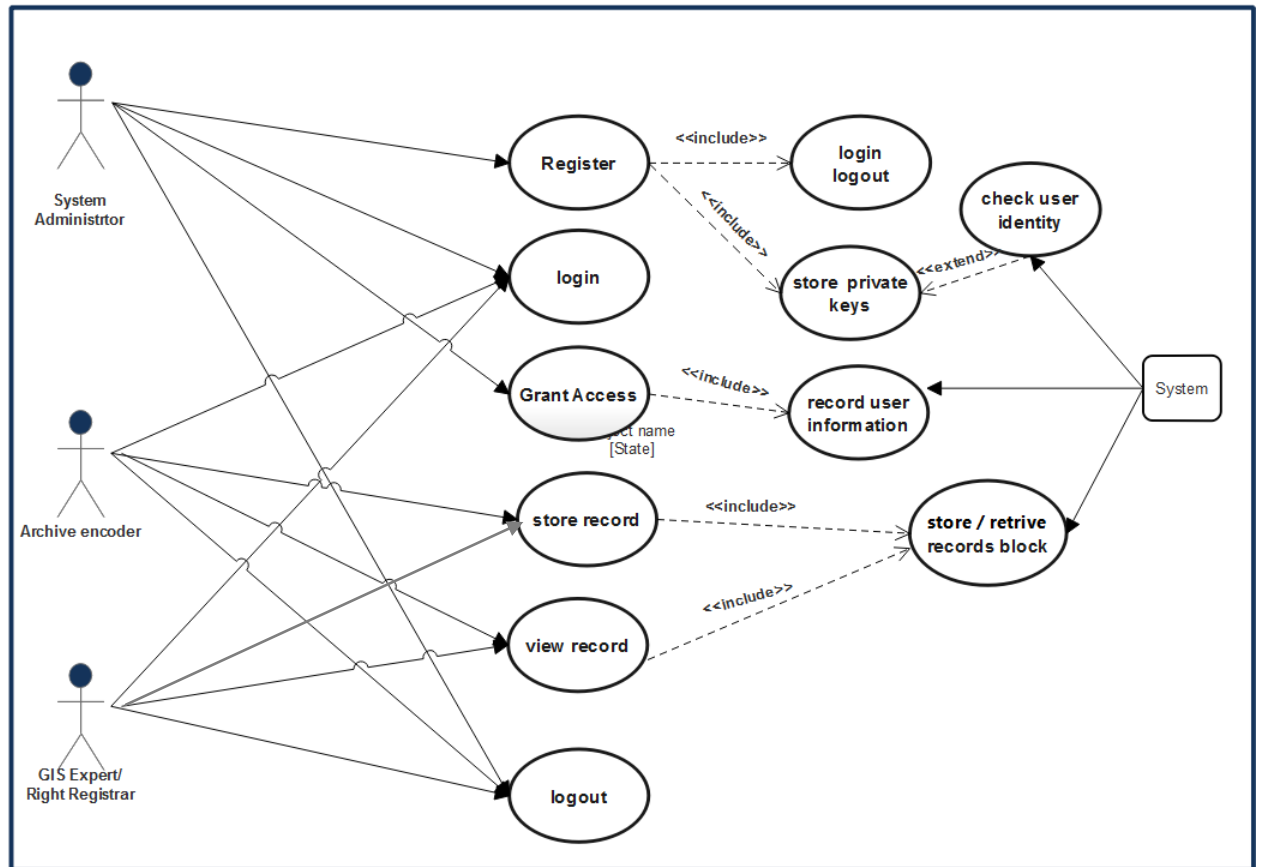


Fig. 4-1 Use case diagram of the system

4.1.5 Use Case Description

1. Use case Name: - User Registration

Participating Actors:- System Administrator, Archive Encoder, GIS Expert, Right Registrar

Description:- the users need to be register in the system

Entry condition: - users have their own secured wallet

Flow of events:- users will be assigned with already available active accounts and register if not they will be assigned

Exit conditions:- users registered successfully

2. Use case Name: - Grant Access

Participating Actors:- System Administrator

Description:- the user accounts need to be granted

Entry condition: - users have their own secured wallet

Flow of events:- users will be assigned with already provide active accounts and privileged accordingly

Exit conditions:- users granted access

3. Use case Name:- Login

Participating Actors:- System Administrator, Archive Encoder, GIS Expert, Right Registrar

Description:- The users need to login to the system

Entry condition: - users have already been registered

Flow of events:- the meta mask extension asks the users to put a valid login credentials if so login accepted and the Dapp will connect to the blockchain.

Exit conditions:-users login successfully

4. Use case Name:- Register Record

Participating Actors:- Archive Encoder, GIS Expert, Right Registrar

Description:- The Archive Encoder needs to register land owner's records

Entry condition: - The Archive Encoder is already registered and logged in

Flow of events:- the user will register and store the record by providing the correct address the hash will be returned to the user and the encrypted data will be stored as a block.

Exit conditions:- the user will logout from the system

5. Use case Name:- View Record

Participating Actors: - Archive Encoder, GIS Expert, Right Registrar

Description:- The users' needs to view registered land owner's record

Entry condition: - The users already registered and login

Flow of events:- View the details of the registered land records from the Dapp and also the block information on the Ganache.

Exit conditions:- the user will logout from the system

4.1.6 Sequence Diagram

Sequence diagrams are used to formalize the behavior of the system and to visualize the communication among objects and to represent the interaction among participating objects in a use case. They are also important to distinguish the missing objects that are not identified in the other analysis objects models.

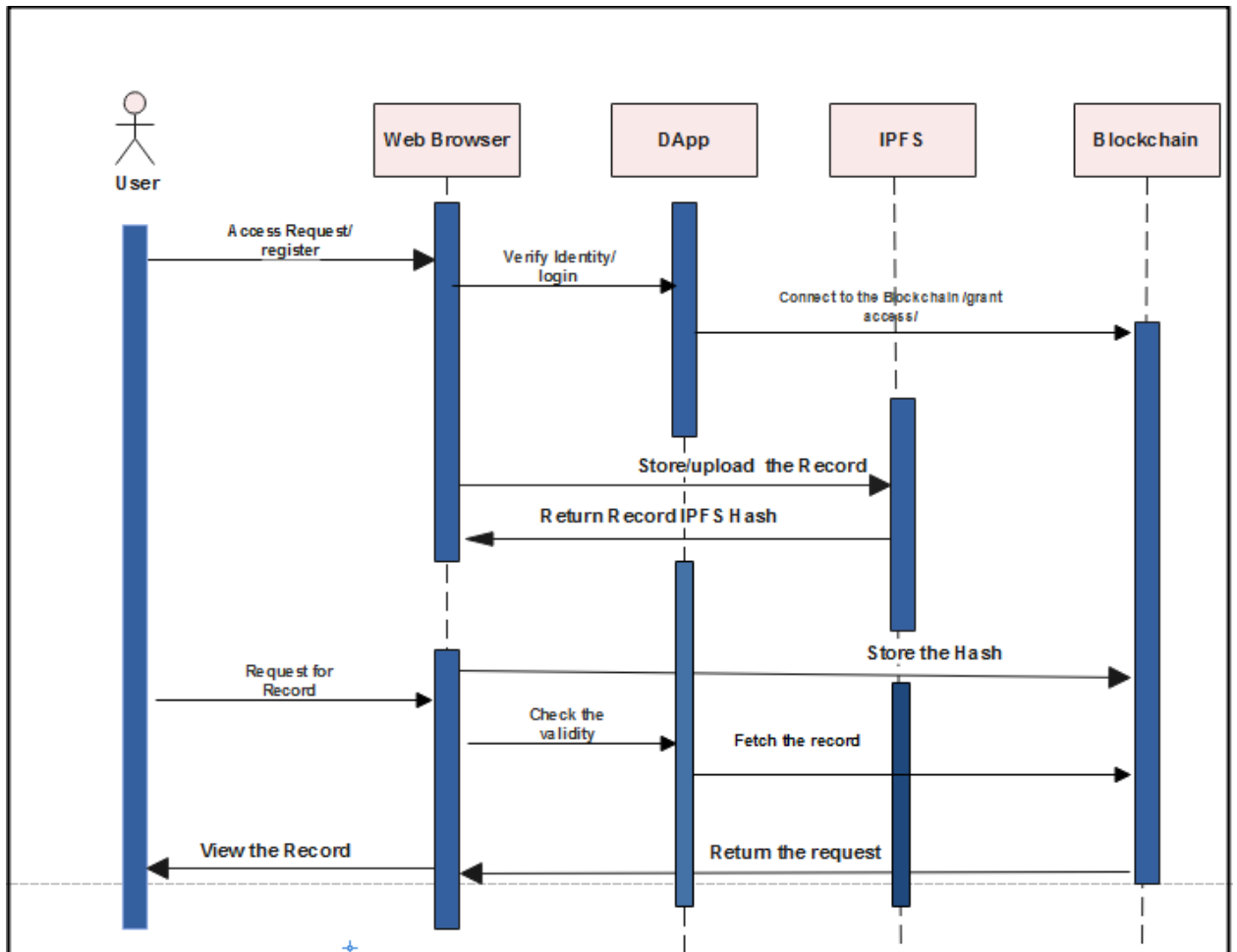


Fig. 4-2 Sequence diagram for the prototype

User first requests to login the system and the system first check if the user is registered to use blockchain enabled browser and a wallet application connected to the browser which is in our case a Metamask. The user provides an account of their Ethereum wallet and after the authentication of the user , the system grant access and allow the user to connect to the blockchain of the Ethereum node in the network.

After the authentication the user will view or store a record. Every stored record will be encrypted by a function of SHA256 then its hash will be stored in the blockchain and then record will be stored in the IPFS.

4.2 SYSTEM DESIGN

System design is the transformation of the analysis model into a system design model. In this section system design components and architecture of the prototype will be discussed.

4.2.1 Proposed System Architecture

The architecture of an application defines how different parts of the system are organized and logically connected. Here the design principles of layered architecture is adopted which is used to designed effective implementation deployment of the blockchain applications and the smart contracts scenarios. Blockchain is a decentralized distributed ledger the application layer is comprised of smart contracts, chain code, and DApps where transactions are arranged in blocks, and placed in a Peer to peer network the other layers ensures that nodes can discover each other and can communicate, propagate and synchronize with each other to maintain valid current state of the blockchain network.

The proposed prototype performs these main actions:-

1. User Registration and Authentication

Participants in the system shall go through a certain process before becoming part of the blockchain system, unlike any ordinary system (client server based system) account creation and authentication is not as such a simple task since every account registered is accountable for saving every transaction in the system so that it becomes a node in the system. But in our case Metamask handles the user registration and authentication.

2. Record Creation and Storage

Each and every record is sent to the Ethereum based blockchain then the blockchain gives the record along with other records a transaction hash which is a SHA 256 checksum of the records passed, these transactions are concatenated and hashed with an unbreakable hash algorithm (SHA256). Records with images (Large files) are saved on the IPFS but hash of names of the files is also sent to the Ethereum blockchain.

3. Record View / Retrieval

On the application interface, after giving user's logging details such as registration key, public key and private key, application will retrieve and display stored records as requested.

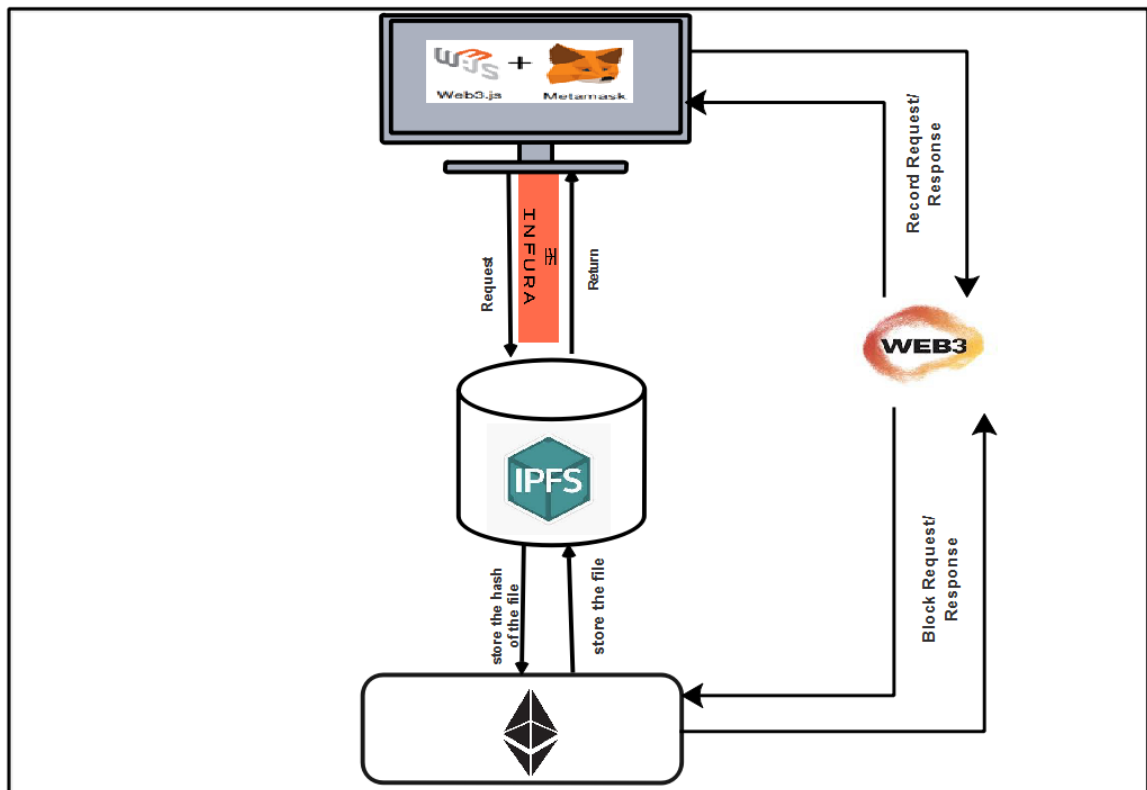


Fig. 4-3 Architecture of the proposed prototype [65]

The user in the client machine that use a blockchain browser with Metamask extension will send request to the webpage then the webpage will be loaded on the browser. After this the client will be able to access the Ethereum Blockchain through Web3 and the block creation of the transaction will be performed as of the client request and the hash will be stored. When clients need to store/ read a record from the system the request will be sent to IPFS through INFURA the user will initialize the IPFS and store a record in which the IPFS obtains the record hash address through SHA 256 algorithm which generates 256bit hash address and the original record will be stored on the IPFS and the reference hash will be stored in the Ethereum Blockchain.

Every transaction in the system shall go through a process called consensus and this is what makes the blockchain special. Consensus in blockchain is achieved by smart contracts and as the name implies they are just contracts prepared for building consensus between two parties and they are smart meaning they don't need human intervention. These smart contracts are written in solidity high-level programming language that let us develop rules

on how records are registered, viewed and edited by the users.

4.2.2 Main Components of the Prototype

The proposed prototype has these main components: -

- **Ethereum Blockchain** – we use smart contracts to the Ethereum blockchain to provide the users to call the smart contract and read/write information on the blockchain also used to store permanent references of each of the land owner in a tamper proof manner.
- **Web3.js** - here the client on the interface will interact with the Ethereum blockchain basically using this API.
- **Web browser** - This component provides a web interface for the users to interact with the application. Users need an Ethereum wallet browser plug-in, namely Metamask to manage their accounts which acts as a bridge between Ethereum Blockchain and the browser.
- **Interplanetary File System (IPFS)** – In this design, since a blockchain cannot store large size data we integrated blockchain with IPFS which is a tamper-proof storage used to store and read records from the network .
- **INFURA-** we used this development suite to provide instant API access to the Ethereum and IPFS networks. It is a hosted Ethereum node cluster that lets users run the application without requiring them to set up Ethereum node or wallet.
- **Client Side Application** – This was developed using React Js which provide an interface to the clients who use a blockchain enabled browser with ethereum wallet and can perform actions as they desired.

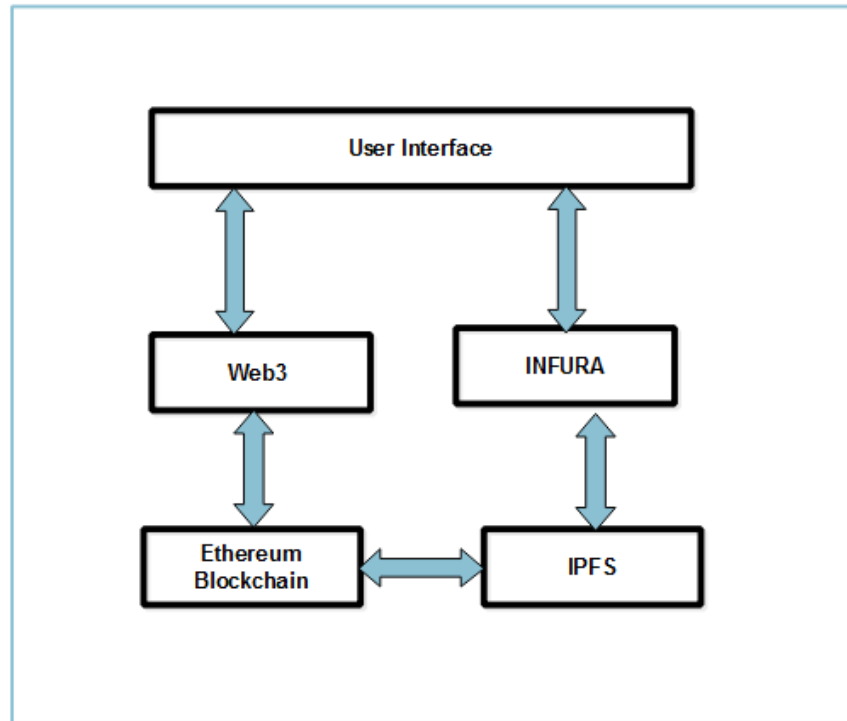


Fig.4-4 Interaction among main components

CHAPTER FIVE

5. IMPLEMENTATION AND EVALUATION

In this chapter the system development tools used for implementing the prototype and the evaluation performed will be discussed.

5.1 IMPLEMENTATION

The implementation part of the system incorporates different development environment which are more powerful the prototype development also different tools and platforms have been used. In the following section presents the tools that are used in the development environment and prototype.

5.1.1 The System Development Environment

Our system is developed using WINDOW 8 64 bit professional operating system, processor Intel® core i3 CPU 1.70 GHZ and 4GB RAM.

Development Tools

These tools are installed and used for the development and implementation of the system.

Table 5-1 Development tools used

No	Tools	Specific Version	Description
1	Node.js	10.16.0	JavaScript runtime environment
2	GIT	2.21.0	Version control system
3	Microsoft Visual Studio c++ build tools	VS2015	Core c++ build tools from version 2015 used for compiling dependencies
4	Python	2.7.18	Programming language
5	Node-gyp	6.2.6	Node

6	Web3.js	1.0.0-beta.46	Collection of libraries that allow you to interact with a local or remote ethereum node using HTTP, IPC or Web Socket.
7	Truffle suite	5.1.50	Blockchain framework
8	Solidity	0.5.16	Programming language used for writing smart contracts
9	Ganache	2.4.0	Local blockchain from truffle
10	Metamask or Brave Browser	—	A browser extension that changes the ordinary browser to a blockchain browser
11	React.js	16.2.2	JavaScript library used for building front-end application development
12	Mocha.js	9.6.7	JavaScript unit testing library
13	Chai	7.4.4	JavaScript assertion library

Remote Systems Used

	Used System	URL	Description
14	Infura	http://infura.io	Access to the Ethereum and IPFS networks
15	IPFS	http://infura.io/ipfs	Inter Planetary File System
16	Remix	http://remix.ethereum.org	Web based application used for testing smart contracts

5.1.2. Setup and Deployment

To setup and deploy this prototype the above tools and dependencies must be installed and each should be accessible by our machine. The DApp which is the front-end system is developed for users to interact with the IPFS and the Ethereum conveniently is developed using ReactJS and Solidity and JavaScript is used for the backend. It has a smart contract named AALHRIAcontract.sol to store the hash of a record. After deployment of the smart contract AALHRIAcontract.sol will get a contract address as its identity and an abstract

binary interface (abi) as the description of the deployed contract and its function.

The contract address and ABI are used in a web3.js library, to allow the interaction between the ReactJS

and the smart contract. This project is deployed using the local blockchain network on the Ethereum Blockchain or the Ethereum Virtual Machine (EVM) however before deploying it to EVM the solidity code is tested on Remix.

After finalizing the setup of Truffle the local blockchain Ganache generates 10 free accounts each with 100ETH and also contain every information like Blocks created and Transaction performed.

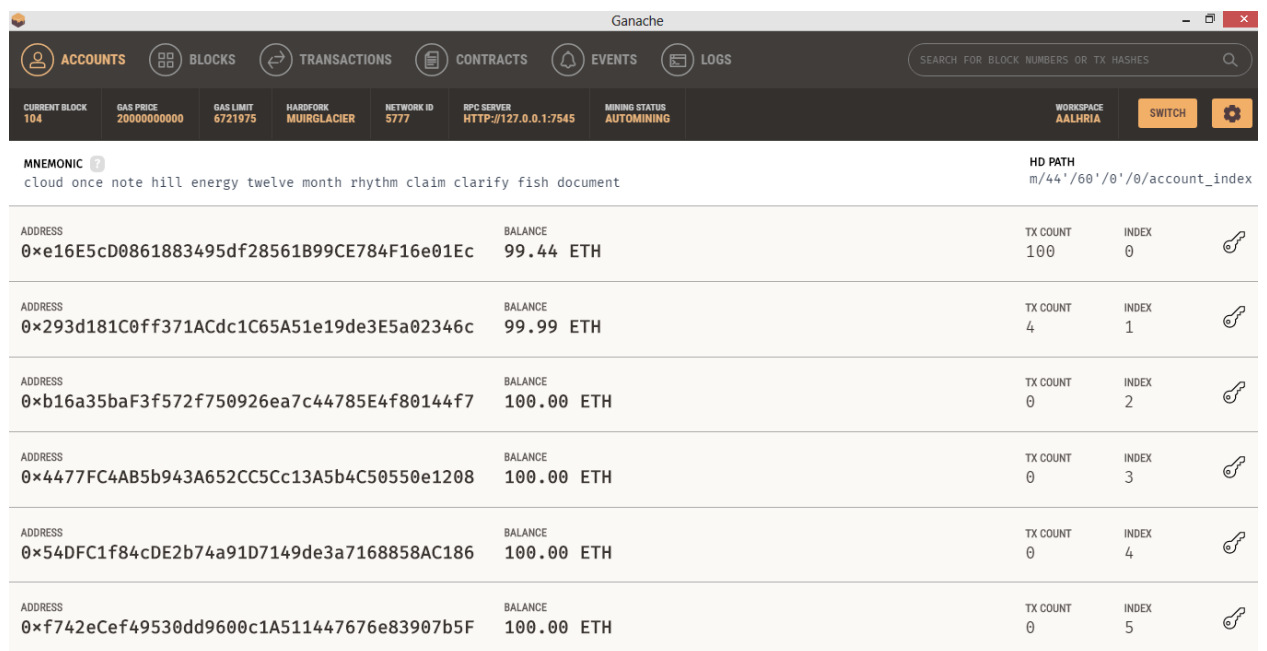


Fig. 5-1 available accounts & address

Ethereum wallet will be used to the authentication of users account the public key which is 42 character long is used as the identity of the user and the private key which is 64 character is used for authentication .

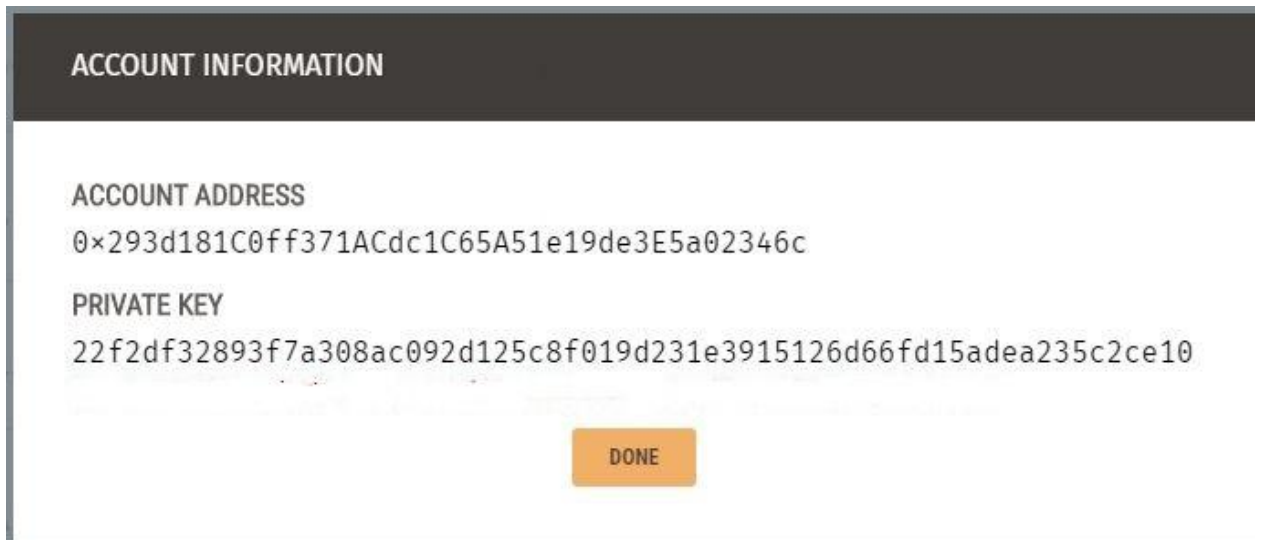


Fig. 5-2 Sample Account

The smart contract compiled using truffle on GitBush console as it's seen in the below.

```
HP@sara MINGW64 /d/SAINT/AALHRIA
```

```
$ pwd
```

```
/d/SAINT/AALHR
```

```
HP@sara MINGW64 /d/SAINT/AALHRIA
```

```
$ truffle compile
```

```
Compiling your contracts...
```

```
=====
```

```
> Compiling .\src\contracts\AALHRIA.sol
```

```
> Compiling .\src\contracts\Migrations.sol
```

```
> Artifacts written to D:\SAINT\AALHRIA\src\abis
```

```
> Compiled successfully using:
```

```
- solc: 0.5.16+commit.9c3226ce.Emscripten.clang
```

After the compilation success the migration of the smart contract will be performed using the command `truffle--- migrate`. Here in shows how the migration process looks like using the command.

```
HP@sara MINGW64 /d/SAINT/AALHRIA
```

```
$ truffle migrate--reset
```


Compiling your contracts...

=====

> Everything is up to date, there is nothing to compile.

Starting migrations...

=====

> Network name: 'development'

> Network id: 5777

> Block gas limit: 6721975 (0x6691b7)

1_initial_migration.js

=====

Replacing 'Migrations'

> transaction hash: 0x9fb28e5a29383ca0b6ee4e10097137934f9cdcc477331575d4495955cb3482a9

- Blocks: 0 Seconds: 0

> Blocks: 0 Seconds: 0

> contract address: 0xF46463FF7a20cdABEF279Ce790a4e16bC542AD87

> block number: 28

> block timestamp: 1610736818

> account: 0xe16E5cD0861883495df28561B99CE784F16e01Ec

> balance: 99.82518176

> gas used: 225237 (0x36fd5)

> gas price: 20 gwei

> value sent: 0 ETH

> total cost: 0.00450474 ETH

- Saving migration to chain.

> Saving migration to chain.

> Saving artifacts

> Total cost: 0.00450474 ETH

2_dapp_deploy.js

=====

Replacing 'AALHRIA'

> transaction hash: 0x84c03d2430be9c17d793b4e50c63642a9bb7b17724ba9321f61dba8261b76c00

```

- Blocks: 0      Seconds: 0
  > Blocks: 0      Seconds: 0
  > contract address: 0xCf2E70465eFcbBAB8829f25E9Be29f3383C3E176
  > block number: 30
  > block timestamp: 1610736822
  > account: 0xe16E5cD0861883495df28561B99CE784F16e01Ec
  > balance: 99.8100984
  > gas used: 711805 (0xadc7d)
  > gas price: 20 gwei
  > value sent: 0 ETH
  > total cost: 0.0142361 ETH
- Saving migration to chain.
  > Saving migration to chain.
  > Saving artifacts
  -----
  > Total cost: 0.0142361 ETH
Summary
=====
> Total deployments: 2
> Final cost: 0.01874084 ETH

```

5.1.3 Prototype Demonstration

The DApp will be available in the address of URL <http://localhost:3000> after running the react development server using the command `npm run start`, the web app will start running on the port 3000. The blockchain enabled browser will ask as the user for a password to the wallet to get connected then it will be redirected to the DApp's home page.

REGISTER

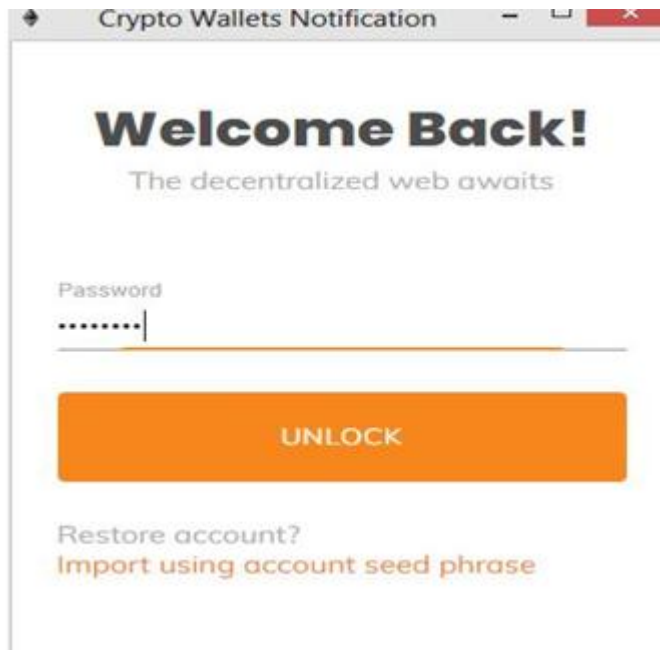
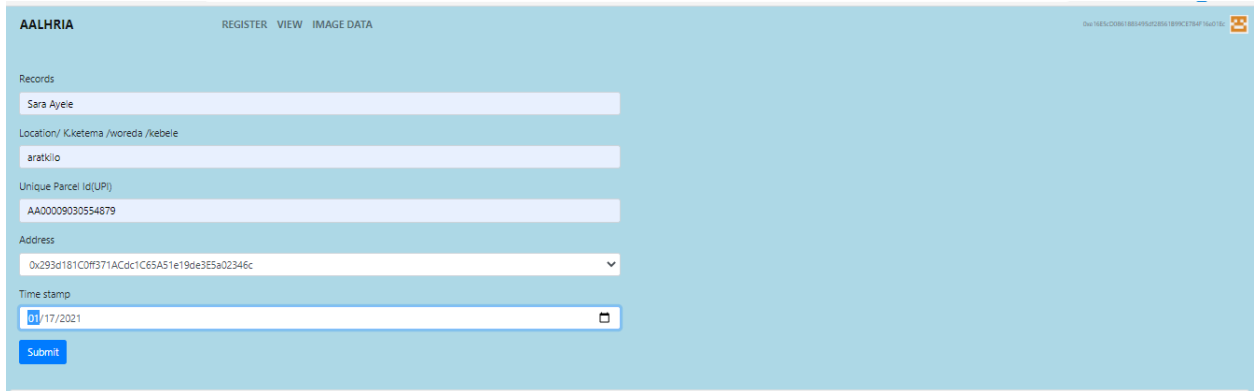


Fig 5-3 Login and home page of the DApp

The home page contains three tabs Register, View and IMAGE DATA for the demonstration of the prototype.

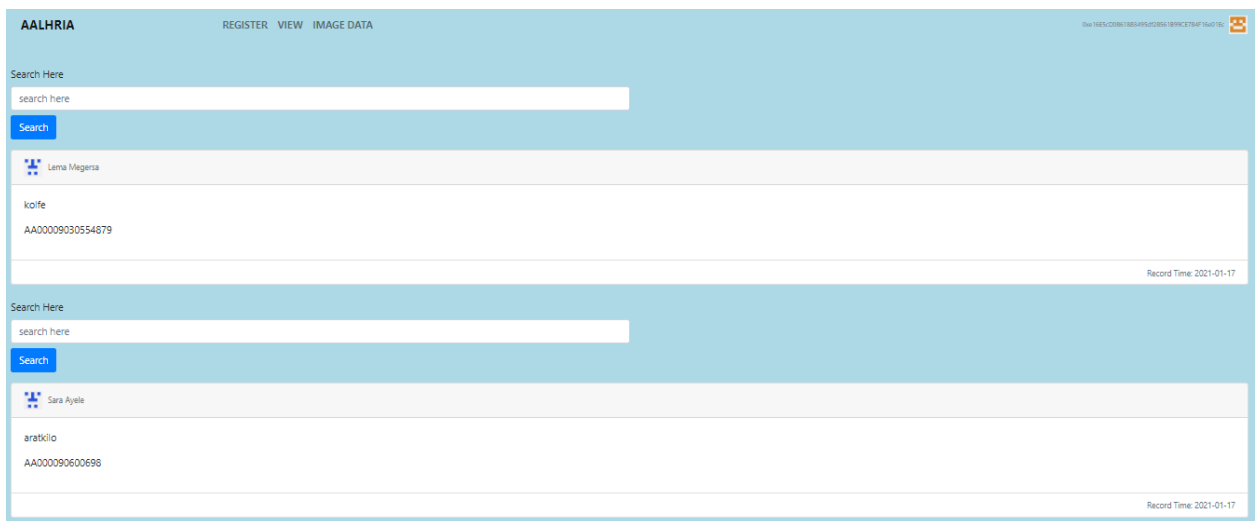
Using the recording tab we will register tenure basic records to a blockchain using the

provided account and the block will be saved in the Ethereum blockchain and every node in the network will have its own copies of all the transactions in the network that make secure the registered record and make sure immutability inside the blockchain.



The screenshot shows a web interface for AALHRIA with a light blue header. The header contains the text 'AALHRIA' on the left, 'REGISTER VIEW IMAGE DATA' in the center, and a small logo on the right. Below the header, there is a 'Records' section with several input fields: 'Sara Ayele' in a text box, 'Location/ K/kefema /woreda /kebele' with 'aratkilo' in a dropdown menu, 'Unique Parcel Id(UPI)' with 'AA00009030554879' in a text box, 'Address' with a hexadecimal hash '0x293d181C0ff371ACdc1C65A51e19ae3E5a02346c' in a dropdown menu, and 'Time stamp' with '01/17/2021' in a date picker. A blue 'Submit' button is located at the bottom of the form.

Fig. 5-4 Registering a record in blockchain



The screenshot shows the AALHRIA view record page. It features a light blue header with 'AALHRIA', 'REGISTER VIEW IMAGE DATA', and a logo. Below the header, there are two search results. Each result has a 'Search Here' section with a 'search here' input field and a blue 'Search' button. The first result is for 'Lema Megerse' with 'koife' as the location and 'AA00009030554879' as the UPI. The second result is for 'Sara Ayele' with 'aratkilo' as the location and 'AA000090600698' as the UPI. Both results show a 'Record Time: 2021-01-17' at the bottom right.

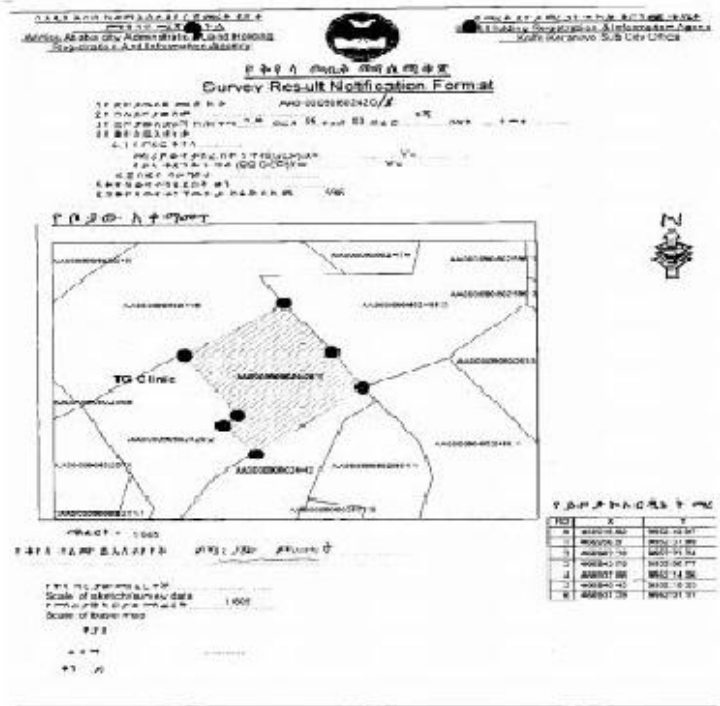
Fig 5-5 View Record page

The IMAGE DATA tab used to attach the necessary scanned image files of a land record as we discussed earlier since the blockchain cannot store larger files the image file will be stored on IPFS and when the Metamask confirm the transaction the respective hash will be returned immediately and the block will be stored on the Ethereum blockchain immediately.

Images No file chosen

Address

0xe16E5cD0861883495df28561B99CE784F16e01Ec



hash of the image: QmavjXCBqRgauZfeNhy'pxoIKkuWlHgA9dJlWT2RXGJZVFrstT

Fig. 5-6 attaching the scanned record

As its shown below every transaction that are executed successfully will be put in a block which contains the Block and Transaction hash all these information.

[← BACK](#) **BLOCK 35**

GAS USED	GAS LIMIT	MINED ON	BLOCK HASH
27363	6721975	2021-01-15 11:46:25	0xb773d9d08f16e4a39993b041ab3eb4d414fae1bedda5caa0af37b4ba67b1c8d5

TX HASH
0x2455ed17f3d892bbf169c009f45877a33cd1a48a1a1d45ae2eb165aa93a59f81

FROM ADDRESS	TO CONTRACT ADDRESS	GAS USED	VALUE
0xe16E5cD0861883495df28561B99CE784F16e01Ec	0x63D7fE59f86EF7b41f8eF4998D4a99B0489c8842	27363	0

Fig. 5-7 Block information

5.2 Testing

Before deploying our project in to the Ethereum Virtual Machine (EVM) we have gone through a testing process by using the available testing tools.

Unit Testing

As we discussed earlier smart contract is a key component of the Ethereum the unit testing is done using on our smart contract using Remix web based IDE.

Remix IDE

Remix IDE is a powerful open source tool that has modules for testing, debugging and deploying of smart contracts and much more.it has a special plugin used to perform unit testing which is called solidity unit testing plugin, by activating the plugin we perform the unit testing for our smart contracts.

Steps followed for the unit testing

- 1) Select solidity environment for Remix IDE home tab
- 2) Provide a directory for the plugin which will be our workspace and will be used to load test files and to store newly generated test files
- 3) Choose the solidity file to be tested AALHRIA.sol and generate
- 4) It uses the library file asserts for testing the solidity files and running the unit testing file it come up with this result for the AALHRIA.sol file of the testing.

As it shown in the figure below the result of the contract in remix unit testing shows 4 passing and 1 failure message on value testing.

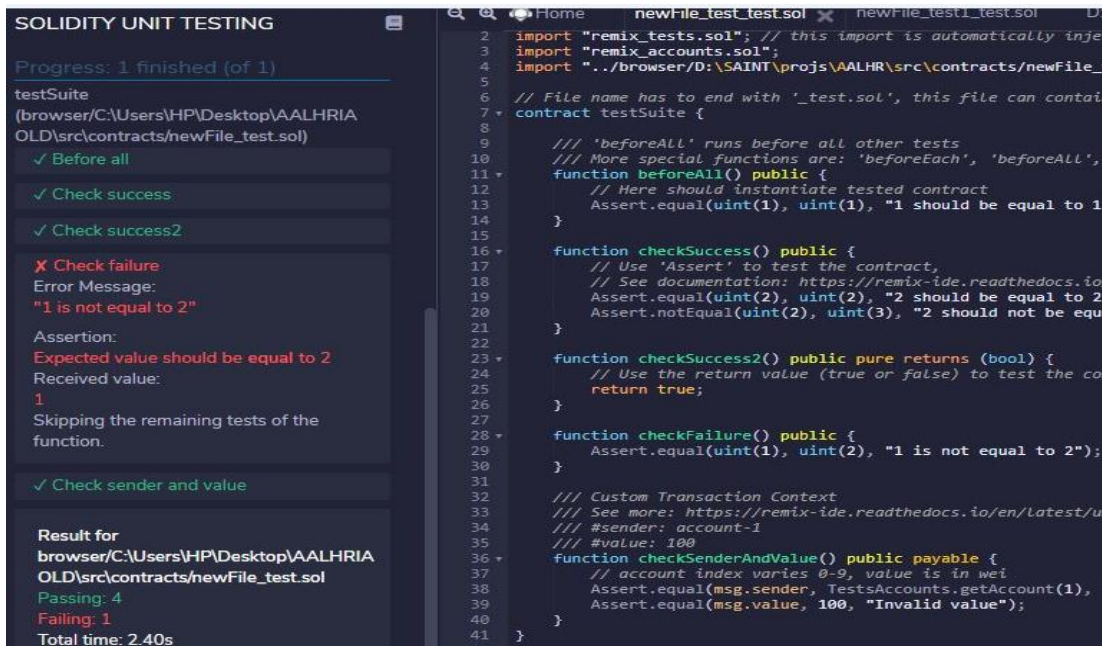


Fig 5-8 Remix unit test result

Integration Testing

Once the unit testing on our smart contract is over integration testing is performed on the interaction between the smart contract and components of the developed prototype by migrating our project in to the Ropsten test networks.

Steps followed

For the integration testing we use the Truffle Framework by configuring it to the Ropsten test network and the command `truffle deploy --network Ropsten` is used to deploy and migrate the project to the test network. After successful migration we did connect to the test network using Metamask plugins and enable us to access the all the components of the prototype fully.

```
Running migration: 1_initial_migration.js
Deploying Migrations...
Saving successful migration to network...
Saving artifacts...
Running migration: 2_deploy_contracts.js
Deploying AALHRIA.sol.
Saving successful migration to network...
```

Fig. 5-9 Deploying on Ropsten network

5.3 Evaluation

The researcher used human expert survey approach to evaluation of the prototype. Even if there are no standardized criteria that we follow to evaluate, we have used points such as usability, impact on users' decision makings and on security issues. The evaluation is done on the usability testing by preparing a questioner to those who have participated while collecting data on the existing system.

The questioner contains total of 10 questions the entire question prepared for system development team members and 6 of them are prepared to be responded by the end users only. Total 31 respondents have participated among them 23 experts of end users and 8 are members from the system development team.

The validity of the system is dependent on the encryption technique used and the hash of the transaction mined on the registration of the records also the feedbacks from respondents who are grouped in to two groups those are the expert of end users officers and experts of the development team used to check the validity and reliability of the result obtained from both groups with different setting. 4.35% of them disagree & neutral about it and 34.7% of them agree and 52.2% strongly agree the system usability which is 86.9% encourage the prototype for further development. From system development team who are participated in the development of the previous system and also on the modification of the security gaps we have got no negative response 12.5% are neutral and 37.5% agree 50% strongly agree which makes 87.5 % of the respondents have a positive feedback on the questioner evaluation of the prototype. Totally from both group of respondents we got an average of

87.2% positive response.

From the evaluation analysis that the respondents from both groups agreed that the system satisfies their main criteria's they were looking a secure way for storing a record which is immutability of a registered record and they gave comments and recommended a more basic attributes fields needed to be further included to the prototype in the future development of the system before deployment. When we see the overall analysis of the respondents' answers we conclude that the prototype is acceptable with the modification of the comments provided by the user in a more large interactive way.

Table 5-2 summary of respondents' score

	Count of Respondents	
	Expert end users	System development team members
Strongly disagree	1	0
Disagree	1	0
Neutral	1	1
Agree	8	3
Strongly Agree	12	4

CHAPTER SIX

6. CONCLUSION AND RECOMMENDATIONS

6.1. Conclusion

This research attempted to answer two research questions. What are the current security challenges being faced by the Agency in managing digitized land records? How can blockchain technology best serve in addressing the existing security challenges? These research questions were answered by adopting a mixed method approach, both qualitative and design science approach.

Problems associated with the existing system were identified through the qualitative research methods (interview, document analysis and observation). Extensive literature review was also conducted to understand how blockchain technology specifically Ethereum blockchain can address the identified problems. Based on these a prototype was developed for the preservation of land records in a more secure environment.

The prototype integrated an Ethereum blockchain and IPFS for storing the image files. The DApp interact with Ethereum blockchain and the IPFS and enable users to register records. The features ensured record immutability because the hashes of registered records can be digitally signed with an Ethereum account and the record as transaction on the blockchain is time stamped and every executed transaction copy is available in every authorized participant nodes.

From the implementation of the prototype and its evaluation, the developed prototype demonstrated that the blockchain can clearly address the security issues on preservation of a record. Also, we believe that integrating and presenting this blockchain prototype will initiate the City Administration to experience on adopting new technology and open a way for others to discover its potential in advance.

6.2 Recommendations

Since this research was conducted on one sector of the City Administration the system should be integrated with systems of other sectors or offices which are engaged in land management related issue to have the complete land management system and for a faster, safer and transparent service delivery. In addition, it is important to prepare standard operating procedures for implementation of blockchain based systems that guides all organizations that work in collaboration with the agency like Courts and Banks. This is because these organizations could access the agency records while passing decisions or addressing mortgage related disputes on owners' assets and notifying the agency.

Here there are some major recommendations for future research:-

- Some improvements is required on the scheme of the prototype to enhance it further by adding all the essential components in the agency business process and can be fully functional in the future as desired.
- Since the technology is in its early stages more research has to be conducted to explore its applications areas and opportunities need to be covered further on the other types of the blockchain.
- Further research can be also conducted in integrating the blockchain with the Artificial Intelligence (AI) for an effective utilization of the technology.
- Integrating the blockchain technology with other existing platforms should be also considered.

References

- [1]. Alfred Menezes, Paul van Oorschot, and Scott Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.
- [2]. Getachew Bayissa, Girum Ketema, Yitagesu Birhanu , "Status of digitization process in selected institutions of Ethiopia", April 2015.
- [3]. International Records Management Trust, "Managing Metadata to Protect the Integrity of Records", May 2016.
- [4]. Martin Harran, William Farrelly, Kevin Curran "A method for verifying integrity & authenticating digital media", Letter kenny Institute of Technology, Donegal, Ireland , 2018.
- [5]. Raquel Benbunan-Fich, Arturo Castellanos, " Digitalization of Land Records: From Paper to Blockchain", Thirty Ninth International Conferences on Information Systems, San Francisco,2018
- [6]. Sangchul Song and Joseph JaJa, "Techniques to audit and certify the long-term integrity of digital Archives".
- [7]. Zerihun Amdemariam Berisso and Tarek Zein, Implementation Practice: "Real Property Registration Systems in Developing Countries: “Confluence of technological, institutional and organizational requirements in the Addis Ababa Project, Paper prepared for presentation at the "annual World Bank conference on land and poverty” The World Bank - Washington DC, April 8-11, 2013.
- [8]. Proclamation No. 818/2014, "A proclamation to provide for registration of urban land holding ", February 2014
- [9]. Victoria L. Lemieux, "Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems: An Archival Theoretic Evaluation Framework", 2017
- [10]. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2009
- [11]. Matti Rossi, Christoph Mueller-Bloch, Jason Bennett Thatcher, Roman Beck, "Blockchain Research in Information Systems: Current Trends and an Inclusive Future Research Agenda" , 2019
- [12]. Vitalik Buterin , "Ethereum white paper a next generation smart contract & decentralized application platform",2013
- [13]. Hartmut MÜLLER and Markus SEIFERT, "Blockchain, a Feasible Technology for Land Administration? ", 2019

- [14]. Stuart Haber, "A Content Integrity Service For Long-Term Digital Archives", HP Labs, Rutgers University, New Jersey U.S.A
- [15]. Gunda Abhishek, "Property Registration and Land Record Management via Blockchains", 2019
- [16]. Albert Galiev, Shamil Ishmukhametov, Rustam Latypov, Nikolai Prokopyev, Evgeni Stolov, Ilya Vlasov , "ARCHAIN: A Novel Blockchain Based Archival System", Kazan Federal University , Russia
- [17]. Hrvoje Stančić, "New technologies Applicable to document and records management:" university of Zagreb Croatia,2018
- [18]. Aanchal Anand , Matthew McKibbin ,Frank Pichel , " Colored Coins: Bitcoin, Blockchain, and Land Administration",2016
- [19]. Nishara Nizamuddin, Haya R. Hasan, Khaled Salah, "IPFS-Blockchain-based Authenticity of Online Publications", 2018
- [20]. IAB Technology Laboratory, "Overview history of BC Blockchain Technology Primer" Version 1.0 | July 2018, <https://www.iabtechlab.com>
- [21]. Abhishek Srivastava, Pronaya Bhattacharya, Arunendra Singh, Atul Mathur, "A Systematic Review on Evolution of Blockchain Generations", ITEE Journal Information Technology & Electrical Engineering, 2018
- [22]. Victoria L. Lemieux, Darra Hofman, , Danielle Batista, and Alysha Joo, , "Blockchain Technology & Record keeping ",Project Underwritten by: ARMA Canada Region, May 30, 2019
- [23]. Dylan Yaga,Peter Mell, Nik Roby,Karen Scarfone, " Blockchain Technology Overview", October 2018
- [24]. <https://www.medium.com /blockchain-architecture-basics-components-structure-benefits- creation>, (Accessed on April 2020).
- [25].<https://www.dragonchain.com/blog/differences-between-public-private-blockchains>, (Accessed on May 2020).
- [26]. Mahendra Kumar Shrivastava, Dr. Thomas Yeboah, "The Disruptive Blockchain: Types, Platforms and Applications", 5th Texila World Conference for Scholars (TWCS), December 2018
- [27]. Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Gautam Das, "Everything you Wanted to Know about the Blockchain", July 2018

- [28]. INTERNATIONAL RECORDS MANAGEMENT TRUST, "Preservation of Electronic Records", Approved by the PRIA Board of Directors on December 19, 2018, www.pria.us
- [29]. Zheng, Z., Xie, S., Dai, H-N., Chen, X. and Wang, H. "Blockchain challenges and opportunities: a survey", 2018
- [30]. Khaled Shuaib, Heba Saleous, Karim Shuaib, and Nazar Zaki, "Blockchains for Secure Digitized Medicine", 2019
- [31]. [https://www. land Blockchain and Land Registration.com](https://www.land Blockchain and Land Registration.com), (Accessed on April 2020).
- [32]. S. Raval, " Decentralized applications: harnessing Bitcoin's blockchain technology", 2016
- [33]. Suyash Gupta and Mohammad Sadoghi, "Blockchain Transaction Processing", May 2018
- [34]. Noe Elisa, Longzhi Yang, Fei Chao, Yi Cao, "A framework of blockchain-based secure and privacy-preserving E-government system", 2018
- [35]. Victoria Lemieux, "Blockchain for Recordkeeping; Help or Hype? ", October 2016
- [36]. Miroslav Stefanović, Đorđe Pržulj, Sonja Ristić, Darko Stefanović, Miloš Vukmanović, "Blockchain and land administration: possible applications and limitations", November, 2018
- [37]. C. Natoli and V. Gramoli, "The blockchain anomaly", IEEE, 2016
- [38]. L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter", 2016
- [39]. A. Castor, "A short guide to Bitcoin forks ", March 2017
- [41]. Zheng Z., Xie S., Dai H., Chen X., Wang H. , "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", June 2017
- [42]. Gupta M. John Wiley and Sons; "Blockchain for Dummies", NJ, USA: 2018
- [43]. Abraham Kelilo Tula, and Firaol Befikadu Geleta , "Building Urban Land Information Management System in PostgreSQL, for the Case of Ethiopia", 2019
- [44]. Blagojevic D. "What is Practical Byzantine Fault Tolerance (pBFT)? ", 2019
- [45]. Sun F. Medium, "A Survey of Consensus Algorithms in Crypto", 2018
- [46]. P Singh 2020, "Role of Blockchain Technology in Digitization of Land Records in Indian Scenario ", 2020
- [47]. Hongzhi Li and Dezhi Han, "A Blockchain-Based Educational Records Secure Storage

- and Sharing Scheme", 2019
- [48]. <http://factom.org>/Antonopoulos, A. (2010)/scalable data layer for the blockchain, (Accessed on January, 2016).
- [49]. Vinay Thakur, M.N. Doja, Yogesh K. Dwivedi, Tanvir Ahmad, Ganesh Khadanga, "Land records on Blockchain for implementation of Land Titling in India", 2019
- [50]. Sam Goundar , "Research Methodology and Research Method", March 2012
- [51]. Hevner, A., March, S.T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research,"
- [52]. Ayanso, A., Lertwachara, K., & Vachon, F. , "Design and behavioral science research", 2011
- [53]. Orit Hazzan, Yael Dubinsky, Larisa Eidelman, Victoria Sakhnini, Mariana Teif, "Qualitative Research in Computer Science",
- [54]. Vaishnavi, V.K. and W. Kuechler, "Design research in information systems. "
- [55]. Syed Muhammad Sajjad Kabir , "METHODS OF DATA COLLECTION" , 2016
- [56]. P. Gill, K. Stewart, E. Treasure and B. Chadwick," Methods of data collection in qualitative research: interviews and focus groups ", 2008
- [57]. Marshall, C. & Rossman, G. B., "Designing qualitative research" Newbury Park, CA:
- [58]. Victor Oluwatosin Ajayi , "Primary Sources of Data and Secondary Sources of Data", 2017
- [59]. John Creswell, "planning, conducting and evaluating quantitative and qualitative research", 2017
- [60]. Roman Beck and Robert Wayne Gregory, "Theory-Generating Design Science Research", 2013
- [61]. Malgorzata Ciesielska, Katarzyna W. Boström, and Magnus Öhlander, "Observation Methods", 2018
- [62]. John Robert Venable, "Design Science Research Post Hevner et al.: Criteria, Standards, Guidelines, and Expectations", 2010
- [63]. Dr. Prabhat Pandey, Dr. Meenu Mishra Pandey, "Research Methodology: tools and techniques", 2015
- [64]. Olga Levina, Marten Schönherr, Udo Bub, "Outline of a design science research process", 2009
- [65]. Intan Permatasari, Meryam Essaid , Hyeonwoo Kim and Hongtaek Ju , "Blockchain Implementation to Verify Archives Integrity on Cilegon E-Archive", April 2020

Appendices

Appendix 1

Interview questions used for employees of AALHRIA for assessing the existing system

1. What is your education level and in which field?
2. What is your Job Title?
3. How much is your land administration related Work Experience?
4. Have you had any experience on the archive system?
5. What security challenges are being faced?
6. How do the challenges being addressed?
7. What methods, tools, techniques are introduced to address the security challenges?
8. What rules, procedures and processes exist to maintain security?
9. How efficient are the existing methods/ tools/ techniques in terms of maintaining security?
10. What are the gaps in the existing processes, methods/ tools/ techniques/ rules/ procedures?
11. How do you think can these gaps be filled with technical solutions?
12. What would you like to be included in the existing system to further strengthen the security land records?
13. What is your overall opinion about the existing system in terms of ensuring security?

Appendix 2

Hello I am SARA AYELE. I am a graduate student in the Department of Computer Science at St. Mary's University. For partial fulfillment of my Master's Degree, I am collecting this information to evaluate the developed prototype I really respect you for taking part in this study. So, after reading the questions carefully, I would sincerely ask you to cooperate with me by feeling it with the following options and providing the necessary information. Thank you.

Strongly Disagree 1, Disagree 2, Neutral 3, Agree 4, Strongly Agree 5

No	Questions	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	Design of the interface in terms colors, reading characters					
2	Is the tools easy to use and accessible					
3	Is it convenient for your service					
4	Did you feel very confident to use					
5	Do you think the prototype contains all the needed components?					
6	Do you need further training to use it?					
7	Do you think the prototype securely store the records?					
8	Is the functions of the systems well integrated					

9	Does the prototype provide more secure environment than the current systems?					
10	Any comment/opinion you would like to add					

Appendix 3

Truffle configuration code

```

require('babel-register');
require('babel-polyfill');

module.exports = {
  networks: {
    development: {
      host: "127.0.0.1",
      port: 7545,
      network_id: "*"
    },
  },
  contracts_directory: './src/contracts/',
  contracts_build_directory: './src/abis/',
  compilers: {
    solc: {
      optimizer: {
        enabled: true,
        runs: 200
      }
    }
  }
}

```

Appendix 4

Solidity code for the smart contract

```
pragma solidity >=0.4.21 <0.6.0;

contract AALHRIA {
    uint256 public recCounter;
    uint256 public imageCounter;

    mapping(uint256 => record) public records;
    mapping(uint256 => imagedata) public imagedata;

    // constructor() public {}

    struct record {
        string ownedby;
        string locate;
        string upi;
        address owner;
        string time;
    }

    struct imagedata {
        string hashval;
        address owner;
        string time;
    }

    function newRecord(
        string memory _ownedby,
        string memory _locate,
        string memory _upi,
        address _owner,
        string memory time
    )
    public {
        recCounter++;
        records[recCounter] = record(_ownedby, _locate, _upi, _owner, time);
    }

    function newimagedata(string memory _hashval, address _owner, string memory time)
    public {
        imageCounter++;
        imagedata[imageCounter] = imaging(_hashval, _owner, time);
    }
}
```

Appendix 5

Sample code for registration of record

```
import React, { Component } from "react";
import Identicon from "identicon.js";
import react from "react";

class Records extends Component {
  constructor(props) {
    super(props);
    this.state = {
      ownedby: "",
      locate:"",
      upi:"",
      address: "",
      timeStamp: "",
    };
  }
  handleChange = (event) => {
    event.preventDefault();
    this.setState({
      [event.target.name]: event.target.value,
    });
  };

  handleSubmit = (event) => {
    event.preventDefault();
    const ownedby = this.state.ownedby;
    const locate = this.state.locate;
    const upi = this.state.upi;
    const address = this.state.address;
    const timeStamp = this.state.timeStamp;

    this.props.newRecord(ownedby,locate, upi, address, timeStamp);
    console.log("you have inserted data" + ownedby, locate , upi , address, timeStamp);
  };

  render() {
    return (
      <react.Fragment>
      <div className="container-fluid mt-5 col-lg-12">
        <form onSubmit={this.handleSubmit} className="inputForm">
          <div className="col-lg-6">
            <div className="form-group">
              <label for="records">Records</label>
            </div>
          </div>
        </form>
      </div>
    );
  }
}
```

```

<input
  name="ownedby"
  value={this.state.ownedby}
  type="text"
  onChange={(e) => this.handleChange(e)}
  className="form-control"
  placeholder="Owner"
/>
</div>

<div className="form-group">
  <label for="location">Location/ K.ketema /woreda /kebele</label>
  <input
    name="locate"
    value={this.state.locate}
    type="text"
    onChange={(e) => this.handleChange(e)}
    className="form-control"
    placeholder="Location"
  />
</div>

<div className="form-group">
  <label for="upi">Unique Parcel Id(UPI)</label>
  <input
    name="upi"
    value={this.state.uip}
    type="text"
    onChange={(e) => this.handleChange(e)}
    className="form-control"
    placeholder="UPI"
  />
</div>

</div>

<div className="col-lg-6 pull-right">
  <div className="form-group">
    <label for="address options">Address</label>
    <select
      required
      name="address"
      className="form-control"
      value={this.state.address}
      onChange={(e) => this.handleChange(e)}
    >
      <option value="0xe16E5cD0861883495df28561B99CE784F16e01Ec">

```

```

0xe16E5cD0861883495df28561B99CE784F16e01Ec
</option>;

<option>0x293d181C0ff371ACdc1C65A51e19de3E5a02346c</option>;
<option>0xb16a35baF3f572f750926ea7c44785E4f80144f7</option>;
<option>0x4477FC4AB5b943A652CC5Cc13A5b4C50550e1208</option>;
<option>0x54DFC1f84cDE2b74a91D7149de3a7168858AC186</option>;
<option>0xf742eCef49530dd9600c1A511447676e83907b5F</option>;
<option>0x7C4cf8DAB84Ef6607B532DDD95493CBDA5723025</option>;
<option>0x50e78Ed0237b9384C7C2096DA3A5eC364E23326B</option>;
<option>0xEEDb2AE997391De654275CF4866aC55921C33958</option>;
<option>0xeb713abfF60B1585611C4Cf3Bd01D2f32012a97e</option>;
</select>
</div>

<div className="form-group">
  <label for="Select Date">Time stamp</label>
  <input
    name="timeStamp"
    type="date"
    value={this.state.timeStamp}
    onChange={(e) => this.handleChange(e)}
    className="form-control"
    placeholder="Date Time"
  />
</div>
<button type="submit" className="btn btn-primary">
  Submit
</button>
</div>
</form>
</div>
<div className="col-lg-12">
  <p>&nbsp;</p>
  {this.props.records.map((rec, key) => {
    return (
      <div className="card mb-4" key={key}>
        <div className="card-header">
          <img
            alt="img"
            className="mr-2"
            width="30"
            height="30"
            src={`data:image/png;base64,${new Identicon(
              rec.owner,
              30
            )}.toString()}` }
        )
      </div>
    )
  )}

```

```

    />
    <small className="text-muted">{rec.ownedby}</small>
  </div>
  <div className="card-body">
    <p>{rec.locate}</p>
    <p>{rec.upi}</p>
  </div>
  <ul id="postList" className="list-group list-group-flush">
    <li key={key} className="list-group-item py-2">
      <small className="float-right mt-1 text-muted">
        Record Time: {rec.time}
      </small>
    </li>
  </ul>
</div>
);
}}
</div>
</react.Fragment> );
}
}
export default Records;

```