TRIBHUVAN UNIVERSITY

INSTITUTE OF ENGINEERING

HIMALAYA COLLEGE OF ENGINEERING

[CT-707]

A

FINAL YEAR MAJOR PROJECT PROPOSAL

ON

REAL ESTATE REGISTRATION SYSTEM USING BLOCKCHAIN TECHNOLOGY

BY:

Ajay Maharjan (HCE075BCT006)

Ashish Rai (HCE075BCT042)

Nibendra Bajracharya (HCE075BCT015)

Sujan Maharjan (HCE075BCT037)

A PROJECT SUBMITTED TO DEPARTMRENT OF ELECTRONICS AND COMPUTER ENGINEERING IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR BACHELOR'S DEGREE OF COMPUTER ENGINEERING

HIMALAYA COLLEGE OF ENGINEERING

LALITPUR,NEPAL

June, 2022

REAL ESTATE REGISTRATION SYSTEM USING BLOCKCHAIN TECHNOLOGY

BY:

Ajay Maharjan (HCE075BCT006)

Ashish Rai (HCE075BCT042)

Nibendra Bajracharya (HCE075BCT015)

Sujan Maharjan (HCE075BCT037)

A report submitted for partial fulfillment of the requirements for the degree of Bachelor in Computer Engineering.

Department of Electronics and Computer Engineering

HIMALAYA COLLEGE OF ENGINEERING

Tribhuvan University

Lalitpur, Nepal

June, 2022

ACKNOWLEDGEMENT

We take this occasion to thank our parents for their consistent support and encouragement. We are immensely thankful to our college, **Himalaya College of Engineering**, for including the project in the syllabus. We are also very grateful for the college for providing us with this opportunity. Furthermore, we extend our sincere and heartfelt thanks to our **Head of Department, Er. Ashok GM,** for providing us with the right guidance and for showing us the right way. We would like to express our deep gratitude towards **Er. Narayan Adhikari Chhetri** as well as other faculty members for their proper guidance and inspiration. Finally, we would like to give special thanks to acknowledge all the people who have helped us towards the development of this proposal.

Group Members

Ajay Maharjan (HCE075BCT006)

Ashish Rai (HCE075BCT042)

Nibendra Bajracharya (HCE075BCT015)

Sujan Maharjan (HCE075BCT037)

ABSTRACT

No country is immune to corruption and the corruption in public offices for private gain degrades people's trust in the government, makes public policies less effective and unreliable. Offices dealing with real estate transaction are no different. It is one of the busiest public offices, with frequent corruption with slow working pace because of tedious record keeping method using paper and centralization. It's important to have records for any kind of property and assets we own, but for an asset like real estate it is imperative to be easily able to prove our claim to the property. The existing property verification and transfer processes are slow, vulnerable to errors, opaque and occasionally corrupt. Using blockchain technology, a decentralized distributed ledger technology which records digital asset with transparency and is immutable, corruption can be minimized, record keeping can be made easier and secured in real estate industry. Deploying Smart Contracts, functionality that comes in Ethereum, a decentralized open source blockchain, the real estate transactions can be automated.

Keywords: *Blockchain, Real Estate, Ethereum, Smart Contracts, Decentralization.*

TABLE OF CONTENTS

Contents

LIST OF FIGURES

LIST OF ABBREVIATIONS

CSS	Cascading Style Sheets
DAPP	Decentralized Application
DB	Database
DFD	Data Flow Diagram
EVM	Ethereum Virtual Machine
HTML	HyperText Markup Language
IPFS	InterPlanetary File System
JS	JavaScript
JSON	JavaScript Object Notation
SDLC	Software Development LifeCycle
OS	Operating System
POW	Proof Of Work
RPC	Remote Procedure Call

CHAPTER 1. INTRODUCTION

1.1. Introduction

Blockchain is a disruptive technology based on cryptography. With the use of blockchain technology many fields such as banks and real estate can benefit from this technology. Real estate is one of the fields in which blockchain can play a vital role. Real estate is a unique and complex asset class. Although the investment market for real estate is huge, it has been dominated by relatively closed network of firms and organizations able to make large investments which are not liquid. Characteristics of real estate such as high transaction cost, land use regulations make the real estate market less efficient. Also, the government bodies which handle the registration of real estate is centralized which makes the record prone to alteration. Blockchain technology could enable the real estate industry to address the inadequacies and imprecisions.

Blockchain is a secure series of timestamped records stored in a database that a group of users manage, who are part of the decentralized network. It is a decentralized or distributed ledger where each node in the network has access to data records stored in the blockchain. The processing takes place within a network of nodes either public or private with a consensus design intended to decentralize authority such that no single source is the sole decider of transactional integrity. Rather authority is decentralized across the operators of the nodes, with each node validating and maintaining verified copies of the ledger. The data records in the blockchain are encrypted using cryptography which ensures the security of the records on the blockchain. No one has the control over the records of data on the chain and it is immutable, cannot be changed even by the person or group of people who created the record. In short, this system of organizing and storing information ensures a number of benefits such as:

- **Immutability**

  Since multiple copies of a block chain are kept and managed by consensus across a peer-to-peer network, no one peer can alter past transactions.

- **Security**

  It is a fundamental crypto-logical law that it is relatively easy to set a problem that is very, very difficult to solve. What is relatively easy for a network of computers to do is, in practice, impossible even for much larger networks to undo.

- **Verifiability**

  The combination of transparency and immutability also allows us to satisfy full public verifiability: anyone in the world can check for themselves that the rules of the system - in the case of digital currencies, that coins should be spent only once - are being followed. Whilst information cannot be manipulated, it can be easily verified thanks to the size and power of the network.

- **Resilience**

  The distributed nature of the ledger makes it resilient. Even if many peers go offline, the information is still accessible.

- **Transparency**

  The fact that all transactions are broadcast to all peers also makes the ledger transparent. However, the encrypted nature of the transactions means that privacy is also assured.

1.2. Problem Statement

In the present state, the entire process of real estate registry maintenance is too tedious since it involves safekeeping of large volumes of registers in written form. The main issue with the above-mentioned method of real estate registry maintenance is that any future reference that needs to be taken from these hard copies will involve too much labor. This process is time consuming. The existing system is not secure since majority of the process is not transparent, system is slow, and selling a property more than once needs to be recorded accurately.

Currently, registration officers and other third party who get involved in a real estate transaction deal often tend to make monetary benefits from the clients who are planning to sell the property. The offline method of initiating a real estate transaction often leads to issues like double spending. Blockchain helps mitigate the interference from third parties by offering a secure platform by means of transaction timestamp, stored within the block.

1.3. Objectives

- To decentralize the record keeping system and increase data transparency.
- To digitize land records.
- To mitigate corruption by real-time accounting.

1.4. Scope and Application

The real estate records are stored by the government in the centralized system, most are paper-based, some are digitized which depend upon the location of the office, but still centralized. Storing records in centralized system is itself vulnerable to forgery and paper-based record keeping is riskier as they can be replaced, can be damaged over time, can be destroyed in accidents, fire for instance. Storing data and records in a centralized system is overall risky and to solve this problem the solution is to decentralize the record keeping system using blockchain which stores data in the chain of blocks, ensures security as each record is hashed using cryptography, provides immutability, transparency. With the features that comes along with the Blockchain Technology, the system is intended for government for recording real estate title and deeds in blockchain.

CHAPTER 2. LITERATURE REVIEW

It is possible to keep track of the property ownership if we have a distributed system which stores all the land history and share it among the interested buyers. This would remove the intermediaries and seller can directly contact the buyer. Thereby removing the extra cost and time that is needed to be spent on the intermediaries [1]. At minimum a blockchain based ledger is needed that stores the transactions done in the process of land ownership transfer. This problem is solved by Satoshi Nakamoto in his paper about bitcoins when he created: [1]

- storing the information in a blockchain,
- for correctness protocol rules can be used,
- and for identifying the owner public key cryptography can be used.

Real estate is a unique and complex asset class. Although the investment market for real estate is huge, it has been dominated by relatively closed network of firms and organizations able to make large investments which are not liquid [2]. Organizing and storing information using blockchain technology ensures benefits such as; immutability, security, verifiability, resilience and transparency [3].

Ethereum is a free open-source platform which helps developers to build and deploy decentralized applications such as smart contracts and other complicated legal and financial applications. Ethereum is kind of a programmable Bitcoin where developers can use the underlying blockchain to create markets, shared ledgers, digital organizations, and other endless solutions application to a problem that need immutable data and agreements, all without the need for a moderator or realtor. Released in 2015, Ethereum is the brainchild of the prodigious Vitalik Buterin, who saw the potential uses of Bitcoin’s underlying blockchain technology as the next steps in speeding the expansion of the blockchain community. Ethereum is now currently the cryptocurrency with the second highest coin market cap and is expected by some to surpass Bitcoin as both a valued investment and as the world’s most popular cryptocurrency. Hence Ethereum is best suited for creating a ledger that stores transactions during the land ownership transfer process. The aim is to create a ledger along with some smart contracts that will triggers the various events that are going to happen on the system during the process of ownership transfer. A Decentralized Application is an application that uses smart contracts providing a friendly user interface to smart contracts. A typical example of DApp is a cryptocurrency application that runs on a blockchain network. A Decentralized application structure is composed by a front-end interface (Web Browser, HTML, CSS) and a back-end interface (Web3 JavaScript). The DApp application interacts with the EVM using JSON RPC. JSON RPC is a stateless and lightweight remote procedure call (RPC) protocol that is used by Ethereum clients to interact with an Ethereum node [4].

For the development of the Decentralized Application the following steps are required [4]:

- Design and implement smart contract in a high-level language (Solidity).
- Compile the contract to generate a binary file.
- Deploy the contract on Ethereum Blockchain network using Ethereum clients (Geth, PyEthApp).
- Build a Web application (Front-end) that interact with the smart contracts. For this use case, the blockchain technology requires two parts:

  – An Ethereum smart contract using Solidity as the programming language which resides on the EVM block.

  – A Distributed App (DApp) composed by front-end and back-end applications in which interacts with the smart contract and the users (landlord/real estate owner and tenants).

The process of signing transactions involves a mathematical function that depends both on the message (the transaction details), and the sender's private key. The result is a signature that can be verified using your public key and the message (the transaction details) [5].

CHAPTER 3. REQUIREMENT ANALYSIS

3.1. Functional Requirements

The functionalities that the system should provide in order to satisfy the needs and requirements of the users are as listed below:

Use Case Diagram

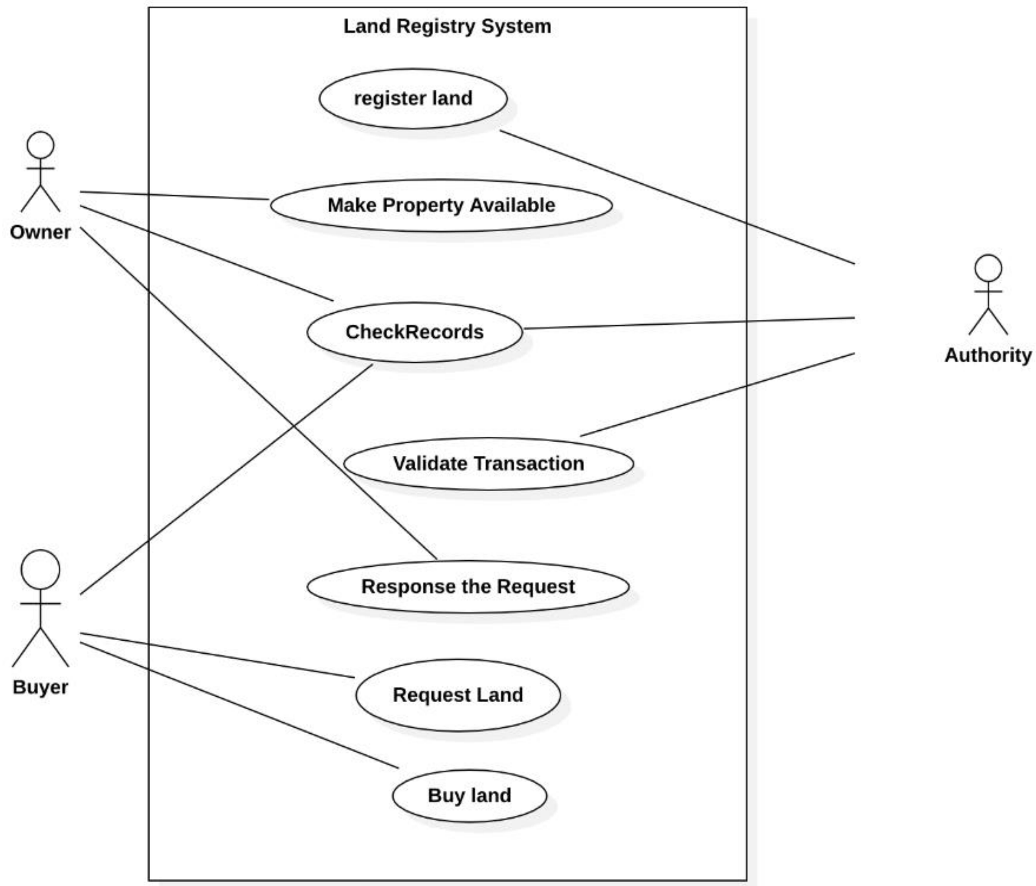

Figure 1: Use case diagram

3.1.1.Register Land

The land owner should be allowed to register their land into the system.

3.1.2. Make Property Available

The system should allow the seller to put the land into sale.

3.1.3. Check Records

The users should be allowed to check records of their transactions.

3.1.4. Validate Transactions

The administration of the system will validate the transactions, after which a new block of record is added into the blockchain.

3.1.5. Response the Request

The users of the system respond to the request made either by accepting or rejecting the requests.

3.1.6. Request Land

The users should be allowed to browse the lands on sale and make request for buying the land.

3.1.7. Buy Land

The buyer can buy land and system will record all those transactions.

3.2. Non-Functional Requirements

3.2.1. Reliability

The system has to be reliable by properly handling unwanted actions or exceptions.

3.2.2. Availability

The system should have uptime to the maximum level.

3.2.3. Performance

The User Interface should be interactive by responding to the actions fast.

3.2.4. Scalability

The system should be capable of supporting the growth and address the concurrent actions.

3.2.5. Maintainability

The system should be maintainable after the deployment.

3.2.6. Security

The system should store the users' credentials securely.

3.3. Feasibility Analysis

3.3.1. Technical Feasibility

The application uses software technologies and tools which are freely available. The technical skills required can be easily manageable. There are many research papers for analysis. The hardware technology required for operation is easy to obtain since the application can run on any computer with a web browser and an internet connection. Since an interactive environment is presented to the user, this system can be used by all kinds of users. So, our project is technically feasible.

3.3.2. Operational Feasibility

This system is operationally feasible as it can run on the computer having minimum hardware specifications, which can run Windows OS or Linux based OS smoothly with an internet connection. No extra hardware needs to be setup to run the system. This system, after it is deployed, can be accessed as a web-based service. So, it can be easily operated to perform the desired functionalities, both by the user and the administrator.

3.3.3. Economic Feasibility

Economic feasibility attempts to weigh the costs of developing and implementing a new system, against the benefits that would increase from having the new system in place. This project can be developed with the help of a computer or a laptop having hardware which can run latest Windows version or Linux OS smoothly. No extra hardware equipment and no expensive software are required for the development of the project. So, our project is economically feasible.

CHAPTER 4. SYSTEM DESIGN

4.1. Software Development Approach

The project will implement the **Incremental Software Model** in its SDLC. It will be developed in multiple increments. In each successive increment, certain portion of the system will be developed. After completion of each increments, testing will be performed to ensure quality of the system.

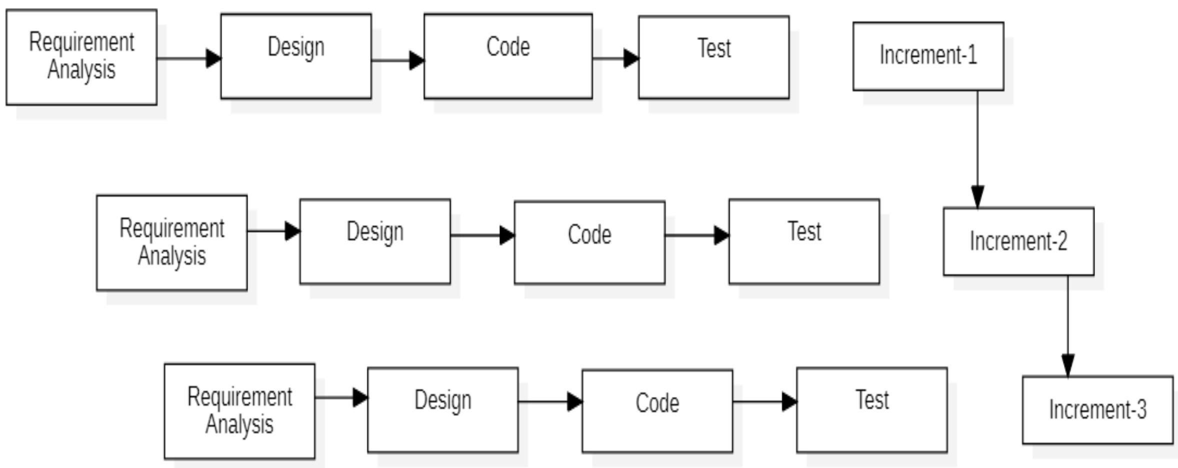

Figure 2: Representation of incremental model

4.2. System Models

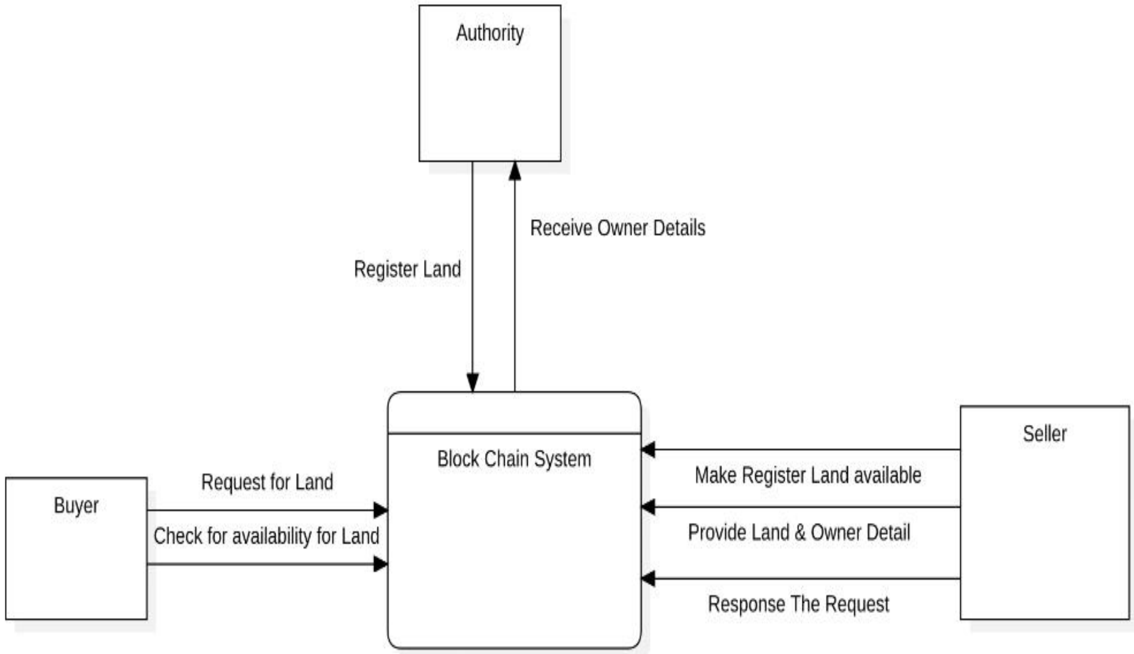

Figure 3: DFD level-0 diagram

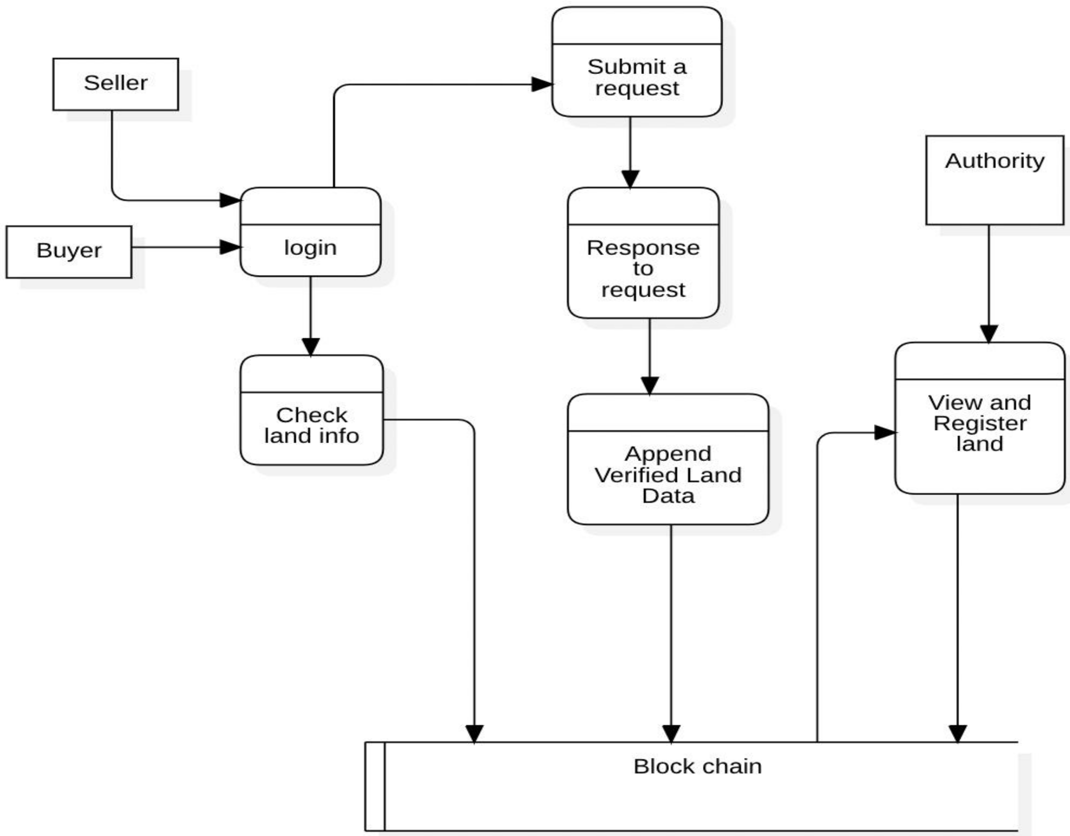

Figure 4: DFD level-1 diagram

CHAPTER 5. METHODOLOGY

5.1. Implementation

The hierarchy involved in organizations involving real estate-based transactions is shown in Fig. 5, which includes one main registration office and associated sub-register offices. Main registration office is linked to the sub-register offices by using previous hash. Main registration office holds data related to original quantity of real estate present before sale while sub-register offices have data regarding amount of real estate which has undergone transaction and the remaining real estate that is available after a particular deal. Users having multiple real estates in multiple states are also kept track off in the chain who are also linked with their respective real estate. Thereby it forms a chain of users with basic transaction related details like the previous and present owner of the property, actual price and selling price of the property along with property size.

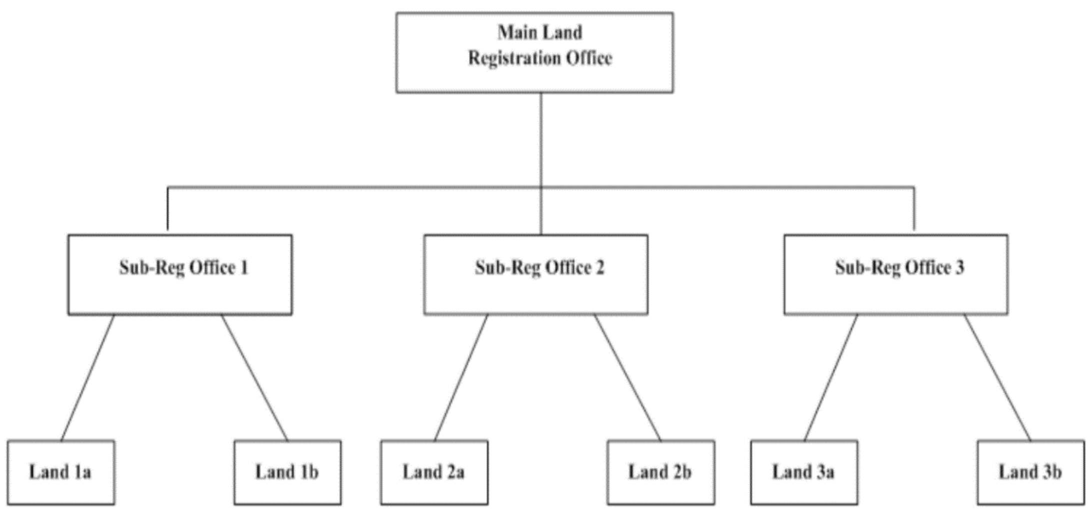

Figure 5: Hierarchy of real estate registration offices

The network is a single main chain, which has multiple blocks linked using hash. Each transaction is verified using Merkle tree. Fig. 6 shows the parameters available within a block associated with an individual user. Parameters at the input and output are used to track our transactions. Input is the point from which all transactions are derived and output is the defined as to whom we are selling the real estate.

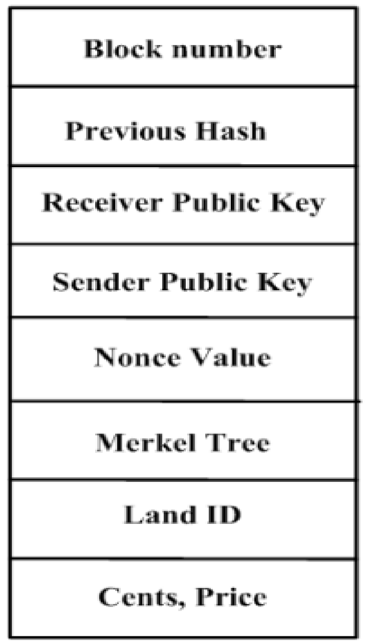

Figure 6: Parameters within a block for a user

Fig. 7 shows the block level details pertaining to multiple users. Public key of each user will be available throughout the network in a distributed manner. Private key will be used by individuals to login to their platform so as to decide on how much real estate must be put to sale and how much money must be transferred to the customers involved. During a transaction, public key will be sent throughout the network for consensus while the private key ensures that the user involved will be able to perform the transaction in a secure manner.

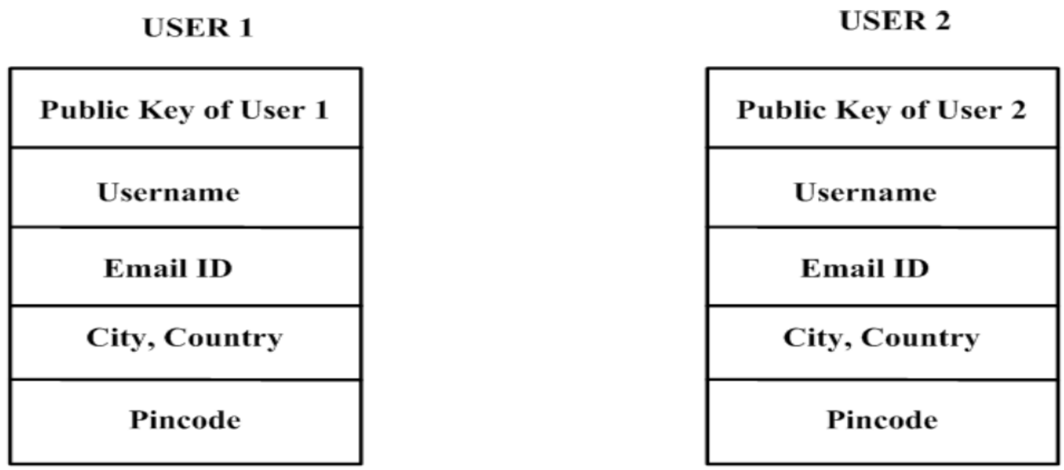

Figure 7: Block level details for multiple users

Fig. 8 shows a real estate transaction that takes place between two users in a blockchain environment. The public key associated with the seller block will be available to the buyer in order to validate the authenticity of the transaction. Private key will be used by individual users to access their data within individual blocks which cannot be accessed by any other person. Fig. 9F shows the case in which only a certain portion of real estate needs to be sold off. The remaining property details remains intact within the user block which ensures reliability. In case of a property which is having more than one owner, transaction happens only when consensus from all the owners are collected. This avoids unnecessary hassle during a real estate deal.

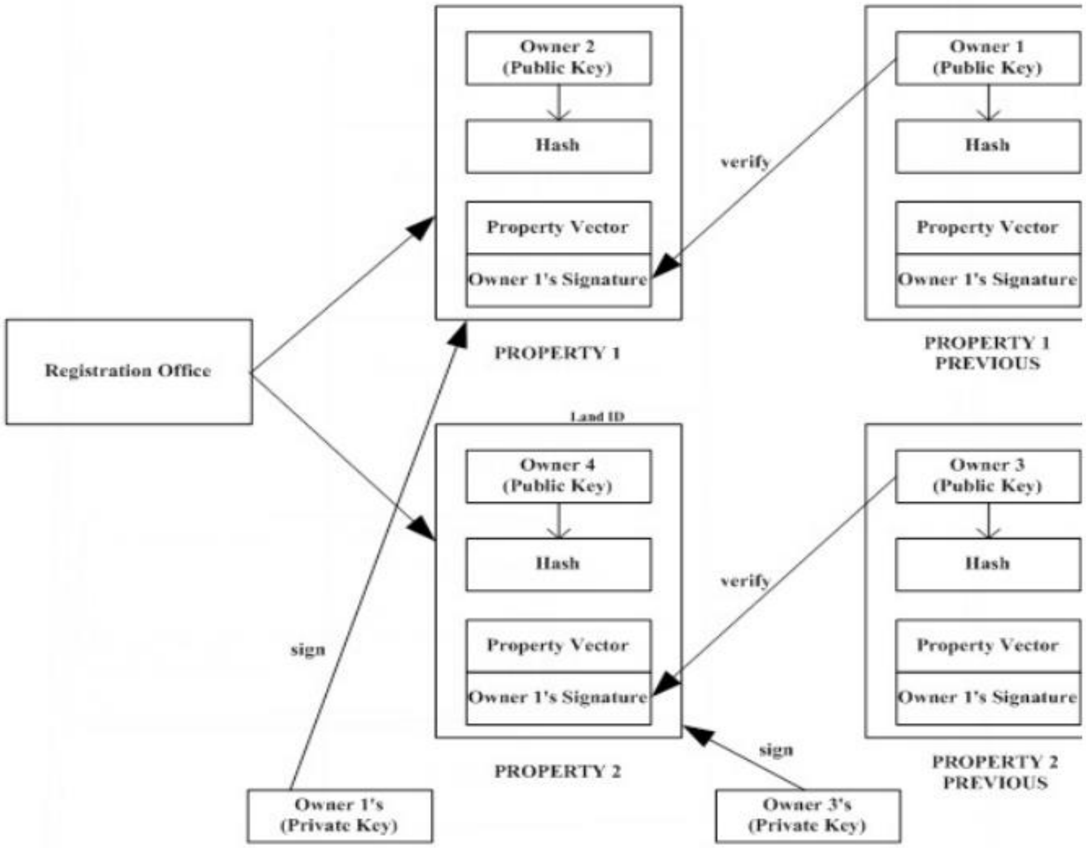

Figure 8: Real estate transaction flow in blockchain

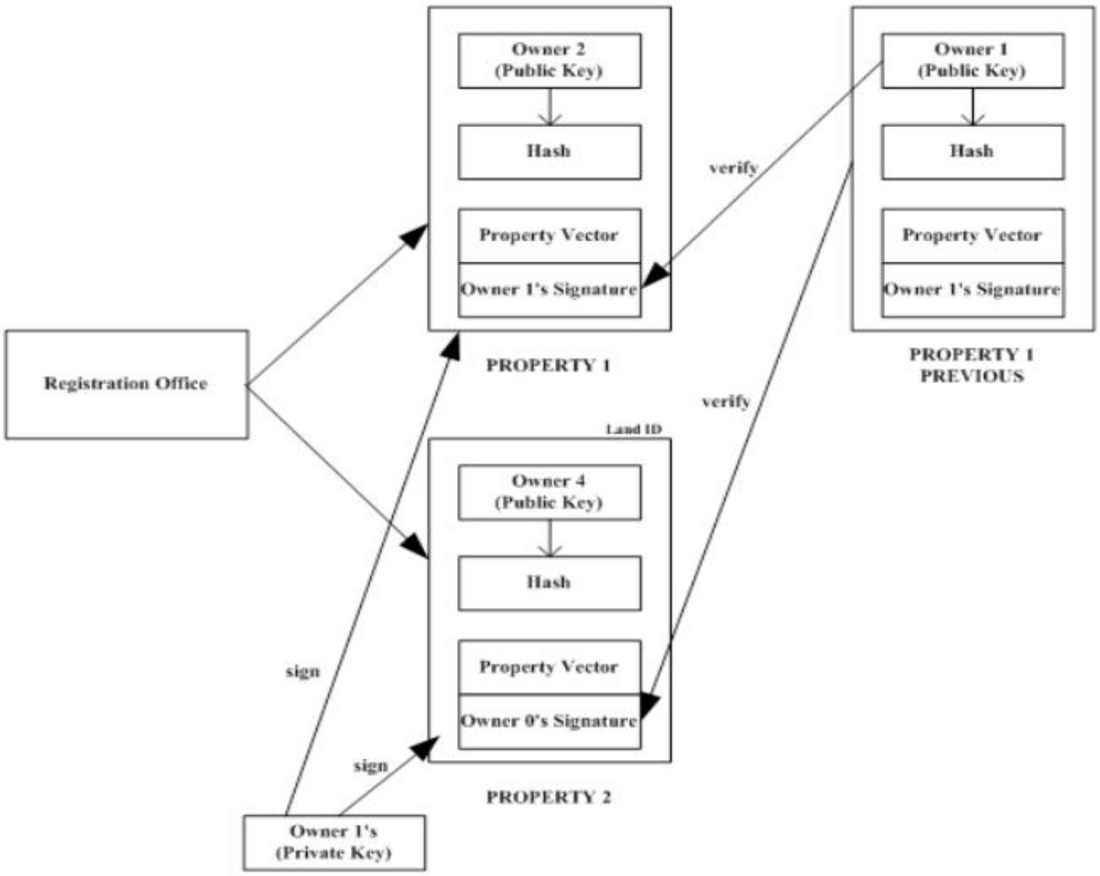

Figure 9: Specialized case of real estate transaction

5.2. Algorithms to be implemented

Algorithm 1 : Algorithm to sell and split real estate

1: function SendRealEstateAlgorithm(senderPrvtKey, estateId, cents, receiverPubKey, price)

2: inputs = get all transaction pointing to the old real estate from the blockchain

3: Find the specific real estate from the blockchain

4: oldRealEstate = getRealEstate(estateId,chain)

5: create new Transaction t(PrvtKeySender, PubKeyreceiver,newreal estate, oldreal estate, inputs)

6: sign the Transaction using the eliptic curve algorithm

st = EdDSA(t,SenderPvtKey)

7: check to see if the transaction was signed by the owner of the real estate itself.

8: distribute the signed real estate for verification to the entire network

9: if (st==signed by owner of real estate) then

10: assert(verifyTranction(t.signature, real estate.owners)

11: else

12: return False

13: end if

14: if (user have real estate to sell) then

15: newRealEstate=split(oldRealEstate,cents)

16: compute hash for new real estate

17: add real estate to blockchain by poW(newRealEstate,3)

18: end if

19: end function

Algorithm 2 : Algorithm for Proof of Work

1: function ProofOfWork(block, difficulty)

2: difficulty factor is 3 zeros in hash value)

3: n = difficulty

4: while (hash(block) != n) do

1. increment nonce value by 1

2. recompute hash

5: repeat step 4

6: end while

7: Otherwise return the block with nonce value

8: end function

Algorithm 3 : Algorithm to add new peer

1: function AddPeer(port)

2: try to connect to a instance on the given port

3: if (connection == TRUE) then

add connection to peer list

4: return True

5: else

6: return False

7: end if

8: end function

Algorithm 4 : Algorithm to transfer data to node

Input the event-type indicating what event it is, message a JSON string representing the contents.

1: function broadcastmsg(eventtype, message)

2: try to connect to a instance on the given port

3: if (connection == TRUE) then

4: for (for all peer in the peerlist) do

send (eventype,msg) to the peer

5: end for

6: else

7: return False

Algorithm 5 : Algorithm to process message

1: Algorithm processmessage (eventtype, message)

2: if the eventtype is connection check to see if connected node has a larger chain if so broadcast(REQUESTCHAIN, null) to connected peer

3: if the eventype is REQUESTCHAIN Create a JSON representation of the blockchain and transmit it to the peer as broadcast(CHAIN, JSON data)

4: if the eventtype is CHAIN convert JSON data to object and check to see if the given chain is valid if the given chain is valid. Then replace the existing chain with new chain

5: if the eventtype is BLOCK download the given block and check to see if all transactions in it are valid by checking the signature against the private-publickeyestate

6: else return false

5.3. Project Tools

The following tools are going to be utilized for the development of this system.

- ReactJS
- NodeJS
- MongoDB
- Solidity
- IPFS

REFERENCES

[1] I. Karamitsos, M. Papadaki, N. B. Al Barghuthi et al., "Design of the blockchain smart contract: A use case for real estateJournal of Information Security," *Journal of Information Security,* vol. 9, no. 03, p. 177, 2018.

[2] V. Chavan and C. Patel, "A study of tokenization of real estate using blockchain technology," *VIVA-Tech International Journal for Research and Innovation,* vol. 1, no. 04, pp. 1-8, 2021.

[3] B. Wigley and N. Cary, "The future is decentralised," United Nations Development Progamme, 2016. [Online]. Available: https://www.undp.org/content/dam/undp/library/innovation/The-Future-is-Decentralised. [Accessed 28 05 2022].

[4] R. Khan, S. Ansari, S. Jain, and S. Sachdeva, Blockchain based land registry system using ethereum blockchain, J. Xi'an Univ. Archit. Technol, 2020, p. 3640–3648.

[5] A. Lymbouras, "A shallow dive into bitcoin's blockchain," [Online]. Available: https://towardsdatascience.com/a-shallow-dive-into-bitcoins-blockchain-part-2-transactions-d4ee83067bae. [Accessed 28 05 2022].