BLOCKCHAIN: DISTRIBUTED LEDGER TECHNOLOGY IN LAND REGISTRY

By- Siva Yogitha Mokkapati

ABSTRACT

The rapid economic growth in India over the past couple of years demand regulatory attention in the property market as this a prerequisite for sustained economic growth. The Government of India is taking more efforts to provide reliable data for efficient delivery of government services. The digital India land record modernization program was launched to bring safe handling of land records with easy access to central repository and real time updates. Although, registration documents can now be submitted via online portal it is not completely automated but is carried out by a team of people in the land registry office. The present system has the following associated problems namely time delay in completing title registration, identifying imposters posing as real sellers of property and human data entry errors.

The transparent nature of blockchain makes it the perfect fit for use in public record systems. The present system of land registration depends on a number of intermediaries including brokers, government property database, attorneys, inspectors, appraisers and notaries. Many time consuming and expensive functions between these entities can be replaced with blockchain and smart contract based automation. The ease and the security of transactions makes blockchain a suitable technology in real estate sector. The use of the blockchain for land registry has the potential to address many of the problems that characterize the typical centralized recording. The decentralization of records with immutable representation of transfer of possession provides opportunity to build a collaborative trustless system. The aim of this project work is to explore the suitability of block chain for its potential to enable "almost instant" transfer of property securely.

The project implementation was carried out in ethereum platform using smart contracts for recording transactions on property transfers and IPFS for secure storage of land documents. The integration of encryption and digital signature schemes provide improved security. A blockchain facilitates decentralization and imposes a constraint that transactions cannot be approved by any single authority but will have to abide by a set of specific rules, thus

enhancing securing. The system permits to add only addition of new blocks since the previous blocks are public they cannot be altered or modified. The properties of blockchain like security, privacy, traceability, inherent data provenance and time stamping makes it vital component for land registry applications. The implementation results clearly brought out the strength of the blockchain in terms of overcoming the mentioned problems associated present online system.

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

IPFS	Inter Planetary File System
DApp	Decentralized Application
PoW	Proof of Work
PoS	Proof of Stake
RSA	Rivest- Shamir-Adleman
SHA	Secure Hash Algorithm
GPG	GNU Privacy Guard
HTML	Hypertext Mark-up Language
CSS	Cascading Style Sheet
JS	Java script
EVM	Ethereum Virtual Machine
RPC	Remote Procedure call
JSON	Java Script Object Notation
EOA	External Owned Account
KDC	Key Distribution Centre
DS	Digital Signature

CHAPTER 1

INTRODUCTION

India has registered rapid economic growth over the past couple of years. One of the areas requiring regulatory attention is a robust property rights system. Land registration is referred to a system used to record and provide information as well as evidence regarding ownership or other rights in land and its related transactions. The government entity is responsible for recording these transactions. Due to a lack of synchronization between agencies handling land records, the information being registered is not standardized. This results in erroneous transactions being recorded (that is rights transferred to a wrong user or boundary violation with respect to land being transacted). In addition, many time's records are not updated correctly. Forgery of land documents has been always reported to be a major problem faced by many state government. Nearly, 1700 cases are registered in the past 8 months across Tamilnadu regarding fraudulent land registrations. Presently, these documents are maintained in centralized databases. The records could be tampered because of no proper security and timestamp. The problem could be solved by blockchain technology, a distributed system that adds blocks with a time stamp and consensus protocol. The blockchain is a recent technology that has received extensive attention which serves as an immutable ledger allowing transactions to happen in a decentralized fashion, thus making it suitable for IT communities and financial service industries.

1.1. Background

In developing countries like India, the problem is twofold. Firstly, securing land documents plays a crucial role in economic development. It addresses economic inequalities and conflict management. Secondly, records are placed in a centralized location. In addition, the existing system is widespread with corruption. A survey conducted by government officials of India showed that approximately 70000 million rupees are being exchanged near the register offices in the form of bribes across India. For the existing architecture, security is created by making systems unapproachable behind firewalls and using other special network connections. The few actors who are involved such as real estate agents, governmental authorities, connect their systems to databases. Blockchain technology facilitates verification of records without jeopardizing the security of the original documents. Other potential risks include a delay in verification of owner, slowed down transactions and land misappropriation. As a result, the Indian government is exploring methods like blockchain to digitize the land records for increasing reliability, authenticity and transparency.

1.2 Problem Statement

To explore the suitability of blockchain for its potential to enable "almost instant" transfer of property securely.

1.3. Specific objectives

S.NO	OBJECTIVE	DESCRIPTION
1	Decentralization	Same digital information is held across a network of computers.
2	Improved security	Overcome fraud and human errors.
2(a)	Fraud	Transactions in blockchain are carried out with digital signatures that provide mathematical proofs and authenticity of the owner. This would stop fraudulent people posing as real owners.
2(b)	Human errors	Since each change is continuously examined by millions of computers in the network the transactions are significantly less vulnerable to human errors.
3	Reduced time delays	The technology could enable instant changes to be made to the information contained on the distributed ledger and title to the property be transferred to the buyer immediately with appropriate time transfer.

Table 1.1: Specific objectives

1.4. Findings

Although registration documents can now be submitted via the online portal it is not completely automated but carried out by a team of people in the land registry office. The present system has the following associated problems namely time delay in completing title registration, identifying imposters posing as real sellers of property and human data entry errors.

The transparent nature of blockchain makes it the perfect fit for use in public record systems. The present system of land registration depends on a number of intermediaries including brokers, government property database, attorneys, inspectors, appraisers, and notaries. Many time consuming and expensive functions between these entities can be replaced with blockchain and smart contract based automation. The ease and security of transactions make blockchain a suitable technology in the real estate sector. The use of the blockchain for land registry has the potential to address many of the problems that characterize the typical centralized recording. The decentralization of records with the immutable representation of transfer of possession provides an opportunity to build a collaborative trustless system.

CHAPTER 2

LITERATURE SURVEY

Land registration is generally defined as a system by which, information relating to ownership and other rights in land can be documented to provide confirmation of the documents, ease transactions and to avoid unlawful deeds.

The main problems associated with existing land registration system are forging documents, not knowing the rightful owner because of improper record maintenance and record loss.

Using blockchain, the above mentioned problems can be solved because blocks are immutable and also blockchain technology is decentralized. The blockchain is defined as a set of blocks that are linked with each other, addressed as the technology of data protection. The linkage is done using hash values and hash functions. These hash values are produced by secure storage systems (e.g. Inter Planetary File System) that store the files and keeps track version of the files. It is peer to peer distributed file system. Whenever a file is stored in this system it returns a unique hash value which is by default the address of that particular file stored. The smart contract helps in creating valid transactions that could be recorded as node information in the blockchain. These contracts can be created using tools like Remix IDE. The remix is an open source tool which helps to write a smart contract in solidity language in the browser. Platforms like ethereum can be used to work with blockchain. Ethereum smart contracts are used to store the origin information of the land which is retrieved from the IPFS file system to the blockchain network to create tamper-proof records pertaining to transactions.

Scenarios of fraud in India that motivated us to take this project

An Article in Hindustan Times, dated on Nov 14, 2017, gives information about 600 crores scam that occurred in Delhi. This scam included officials of Delhi and the mafia. The Delhi officials faked the land documents with the help of fake court orders to transfer at nearly

30 acres of government property, which is worth over Rs.600 crore to private individuals. Fig 2.1 shows how the scam has happened. This scam is considered as one of the biggest scams in India till date.

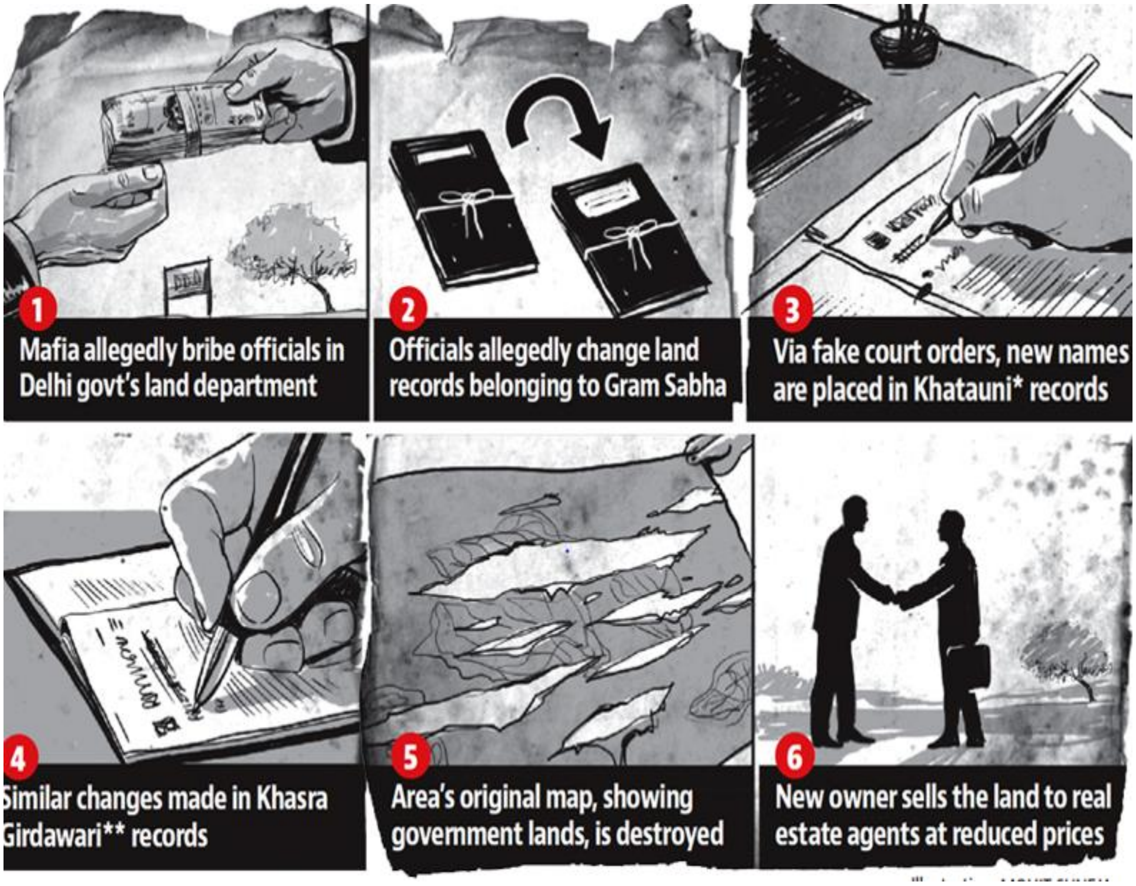

1
Mafia allegedly bribe officials in Delhi govt's land department
2
Officials allegedly change land records belonging to Gram Sabha
3
Via fake court orders, new names are placed in Khatauni* records
4
Similar changes made in Khasra Girdawari** records
5
Area's original map, showing government lands, is destroyed
6
New owner sells the land to real estate agents at reduced prices

Fig 2.1: Fraud Scenario

Link: https://www.hindustantimes.com/delhi-news/rs-600-crore-property-scam-unearthed-in-delhi-cbi-asked-to-probe/story-FXNlgBOgJwSi328HJCwuiM.html

Another scenario dates back to 5th may, 2015 in which a seller sold a property for a certain amount of money and gave fake documents to the buyer. The buyer paid him the total amount and went to the sub-registrar to verify the papers and then he came to know that the papers were fake.

Link: https://www.legallyindia.com/forum/7-legal-issues-talk-and-help/4165-illegal-transfer-of-property-by-forgery-impersonation

In the above mentioned scenarios, the problems are mainly because of forging documents or because of not knowing the owner.

Using blockchain one can solve these because blocks are immutable and also because blockchain is decentralized.

Land registration

In the existing land registration procedure referred in Fig 2.2, the buyer and seller after negotiating submit the entire set of documents that are to be registered with the registration clerk at the registrar office. Verifier in the registration office will verify the authenticity of the documents and gives a token number to them. The computer operator, will enter the required information in the registration software and then take the photo and thumb impression of both parties along with witnesses. Parties will then sign print in front of the Registrar and returns it back. Payment of registration fees will be done by them and the Registrar will sign the final document. The signed hardcopy of the same is given to the transactor as proof of successful transaction completion.

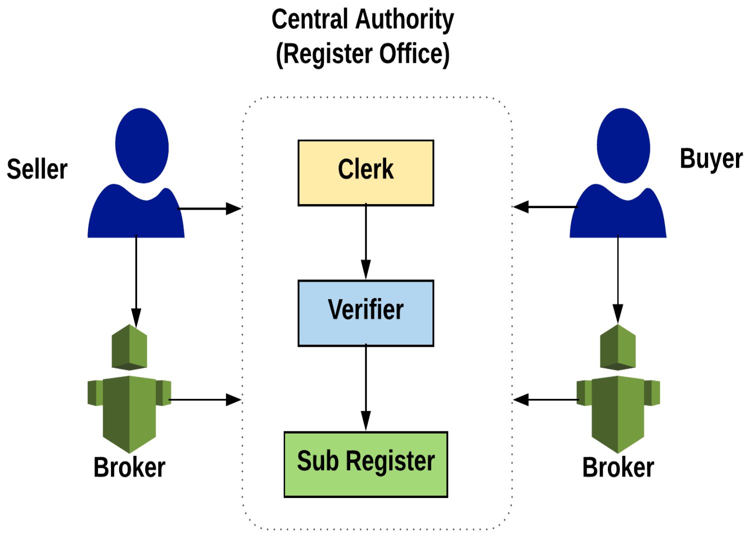


Fig 2.2: Existing land registration system

Problem with existing land registration system:

1. Most of the process is not transparent. Hence, stakeholders cannot know what is happening.

2. The system is slow at registering real estate transactions that are the time from purchase till legal approval takes 3-6 months.

3. All the stakeholders like a buyer, seller, and brokers should create their own complex processes for agreements between them since they have to make sure that things can't go wrong, and because the value of the transactions is large.

Blockchain technology

A blockchain technology is referred to a distributed cryptographic system which identifies and stockpiles an immutable, consistent log of transactions that happens among interconnected actors. In a network, blockchain imposes transparency and guarantees eventual, system-wide agreement upon the validity of the history of transactions. In addition, blockchain technology ensures that transactions complies with the programmable procedures in the formation of "smart contracts".

Platforms for blockchain technology can be categorized into two types:

1. Public platform: Where anyone can read and write that is permission less.
2. Private platform: It allows different permissions to be defined on different users of the network. Depending upon the operations there can be various types of authorization on the blockchain.

PLATFORM	**Public**	**Private**
With smart contract	Ethereum	Hyperledger
With cryptocurrency	Bitcoin	Multichain

Table 2.1: Blockchain platforms

The constituents underlying the blockchain consists of blocks, consensus, smart contract, transactions and applications which are divided into different layers which we call the blockchain ecosystem. The layers are a network, transaction, the blockchain, trust, application and security layers. The network layer indicates a P2P network with the Ethereum nodes. The transaction layer discusses the transactions activated by a smart contract. The Blockchain layer is utilized to refer to block status which contains all the necessary information. The trust layer talks about the consensus protocol for block and transactions validation. The application layer covers applications, state machine, and smart contract. The layers of blockchain are shown in Fig.2.3.

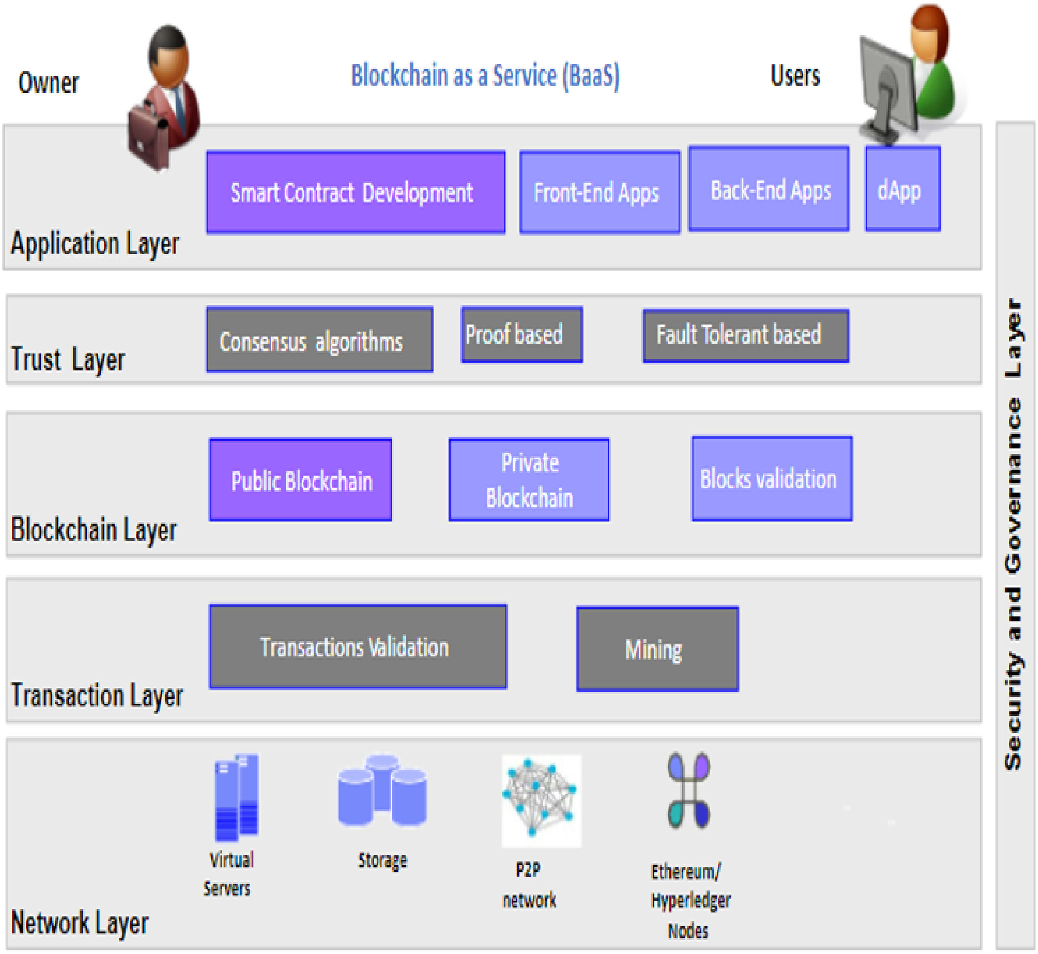


Fig.2.3: Layers of the blockchain

Blockchain - Development phases

Designing and implementing blockchain applications requires analysis, design and implementation phases. The requirements of the application are collected and analyzed during the analysis phase. Identification of the parties and entities involved is also part of analysis phases. During the design phase, the entity attributes and interactions between them are modeled as functions. The implementation of a smart contract for blockchain is done during the implementation phase. The constituents of the smart contract are functions, modifiers, state variables, events in Solidity. DApp is mandatory if a user-friendly UI is required. Fig 2.4 shows the development phases of the blockchain.

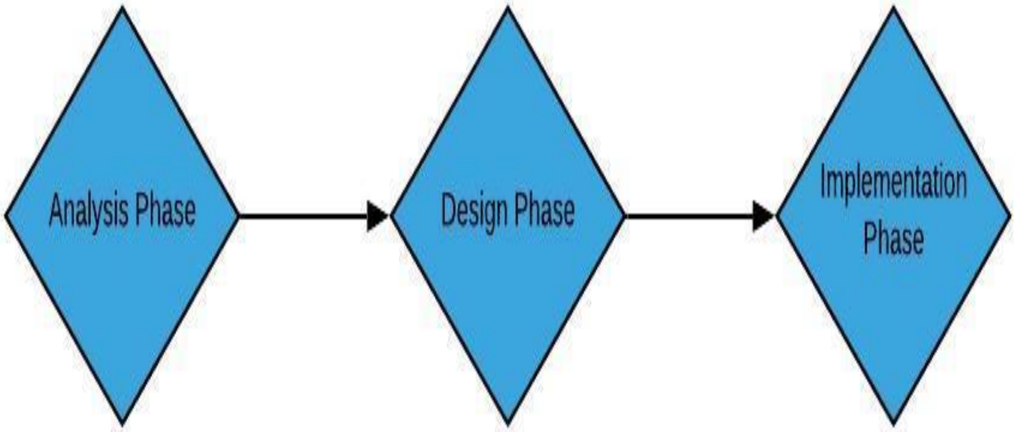
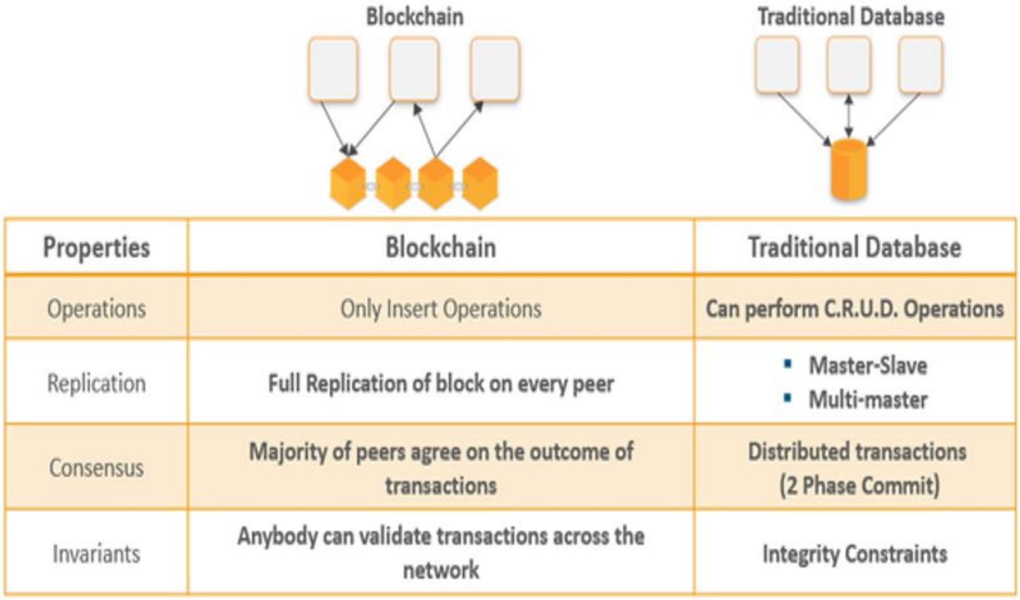


Fig 2.4 Development phases of the blockchain

Blockchain versus Traditional databases

The key differences between blockchain and traditional databases are shown in table.2.2.


Blockchain
Traditional Database

Properties	Blockchain	Traditional Database
Operations	Only Insert Operations	Can perform C.R.U.D. Operations
Replication	Full Replication of block on every peer	▪ Master-Slave ▪ Multi-master
Consensus	Majority of peers agree on the outcome of transactions	Distributed transactions (2 Phase Commit)
Invariants	Anybody can validate transactions across the network	Integrity Constraints

Table:2.2: Blockchain vs traditional databases

Features of blockchain

Centralized system vs decentralized system

Centralized system:

Centralization can be termed as a hierarchical level within an organization that has the authority to make decisions. In simple terms, if decision making is kept at the top level, the organization is said to be centralized (that is the holding of authority and powers with respect to planning and decisions making will be with the higher authorities). Structure of the centralized system is shown in Fig.2.5. The system contains a systematic and consistent reservation of authority. The communication flow is vertical. Coordination and leadership will be proper. However, the time for decision making will be relatively slow and the control of decision making lies only in the hands of higher authorities of the organization.

It is suitable for small scale organizations. It increases the work consistency and efficiency along with reducing the costs.

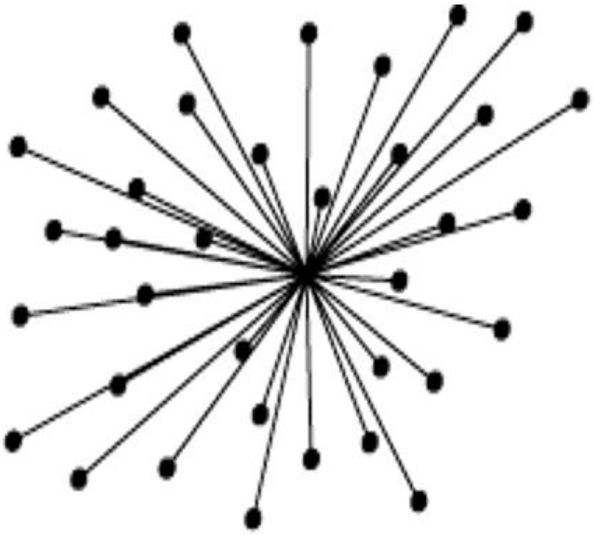


Fig.2.5: Centralized System

Decentralized system:

The distribution of control (authority and responsibility) by the top administration to a low level or middle management is known as Decentralization. In simple terms, it is the designation of authority, to all the levels of the organization. It is the contrary of centralized system, wherein decentralized system the power of decision-making is given to the divisional, departmental and central level administrators, organization-wide. It is also referred to as an addition to the allocation of authority. The structure of the decentralized system is shown in Fig 2.6.

Decentralization involves a systematic dispersal of authority. The communication flow is free and open. The workload and responsibilities will be equally shared among all the available staff, which is the key advantage of the decentralized system over a centralized system. Decision making time comparatively faster in the decentralized system when compared to a centralized system as multiple persons are involved. It is the best fit for large scale organizations.

However, decentralization lacks leadership as well as coordination, which may lead to ineffective control over the organization. For a decentralization process to be effective, open and free communication is compulsory.

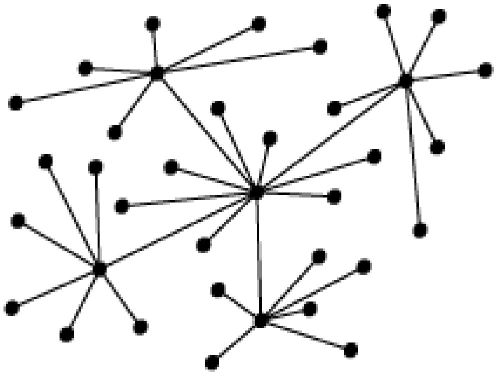


Fig 2.6: Decentralized System

The key differences between centralization and decentralization are listened in Table.2.3 and diagrammatically shown in Fig 2.7.

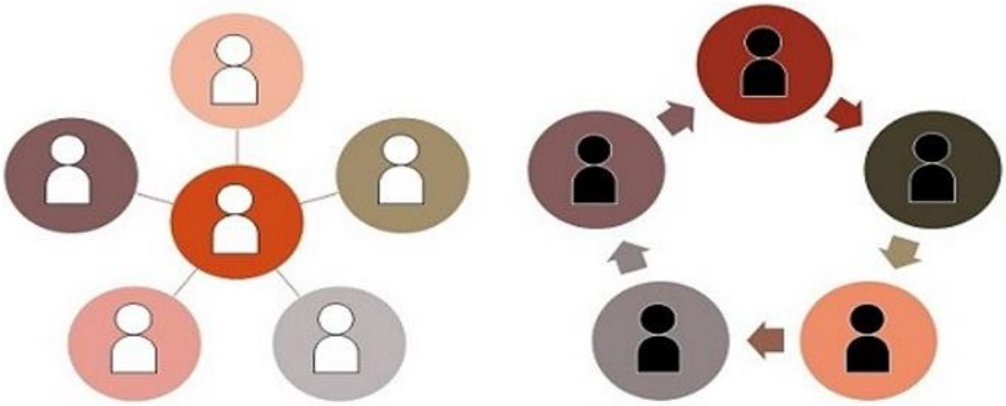
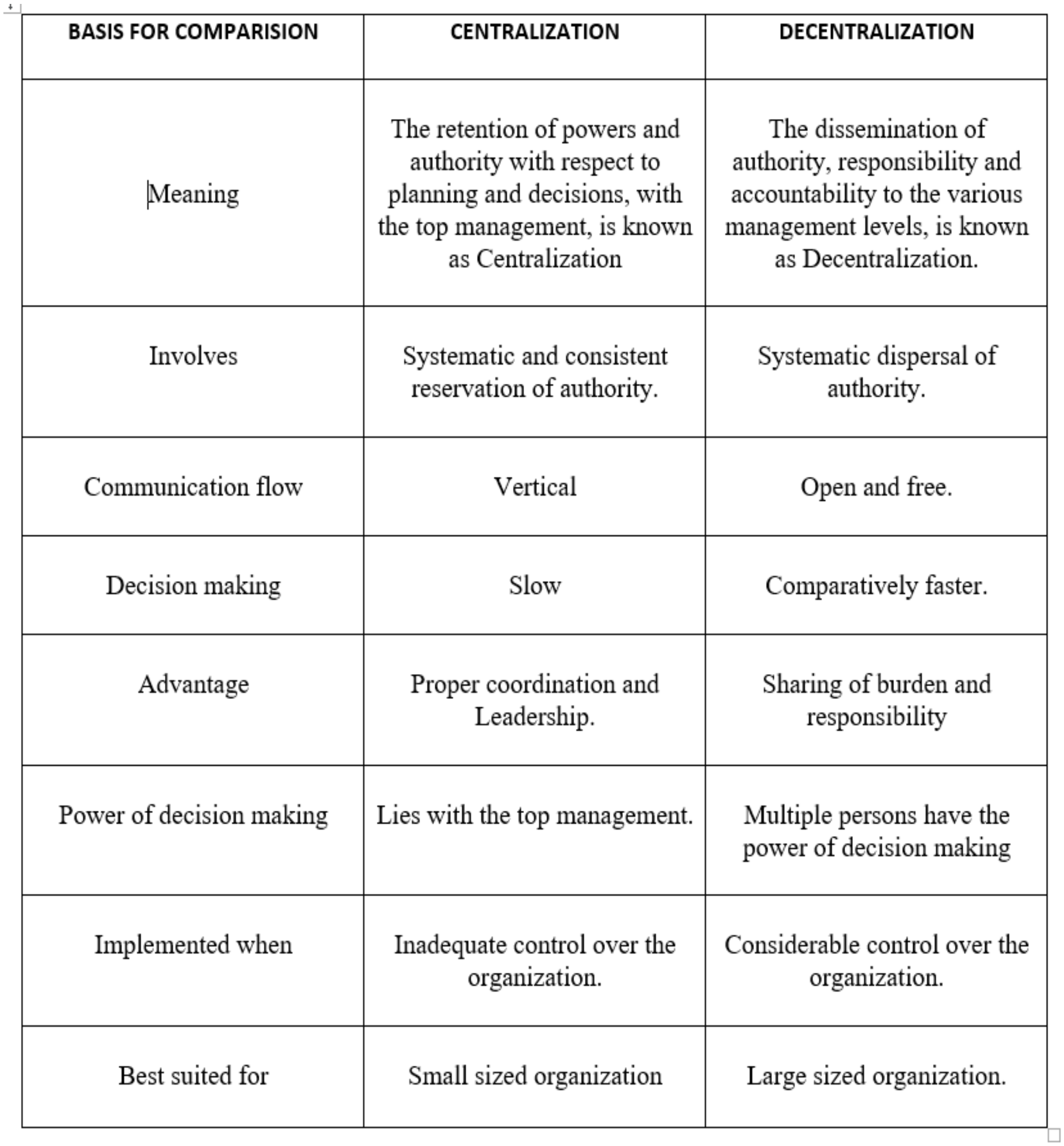


Fig 2.7: Centralization Vs Decentralization



BASIS FOR COMPARISION	CENTRALIZATION	DECENTRALIZATION
Meaning	The retention of powers and authority with respect to planning and decisions, with the top management, is known as Centralization	The dissemination of authority, responsibility and accountability to the various management levels, is known as Decentralization.
Involves	Systematic and consistent reservation of authority.	Systematic dispersal of authority.
Communication flow	Vertical	Open and free.
Decision making	Slow	Comparatively faster.
Advantage	Proper coordination and Leadership.	Sharing of burden and responsibility
Power of decision making	Lies with the top management.	Multiple persons have the power of decision making
Implemented when	Inadequate control over the organization.	Considerable control over the organization.
Best suited for	Small sized organization	Large sized organization.

Table: 2.3: Centralization Vs Decentralization

Reasons for decentralization in blockchain:

1. Users empowerment

   Because of the system being decentralized, the information and transactions related to users are controlled by the users itself.

2. Fault tolerance

   If a system is decentralized, it is less likely for the entire system to fail as they rely on many separate systems

3. Resistance to attack and durability

   Since there is no central authority or control, chances of surviving from a malicious attack are high that is it is more expensive to attack, manipulate or destroy a decentralized system.
4. Scam free

   Users of the decentralized system cannot indulge kind of scams.
5. Higher transaction rate

   Transaction sped is very high in blockchain that is a transaction can be processed in minutes using blockchain. In comparison, the existing ways through which transaction happens via banks take much longer time for processing.
6. Lower transaction costs

   Blockchains have the capability to reduce transaction fees. Also, the overhead costs for exchanging properties is reducing because of the decentralized system.
7. Transparency

   Any change to public blockchains can be viewed publicly by all parties. Also, the transactions are immutable, that is it cannot be changed or deleted.
8. Authenticity

   Because blockchain is the decentralized system, the data in blockchain is complete, consistent, timely and accurate.

Distributed System

A distributed system is referred to as a network that contains an autonomous number of computers that are connected using a distributed middleware. They provide users with a single and integrated coherent network by sharing different resources and capabilities. The structure of the distributed system is shown in Fig 2.7

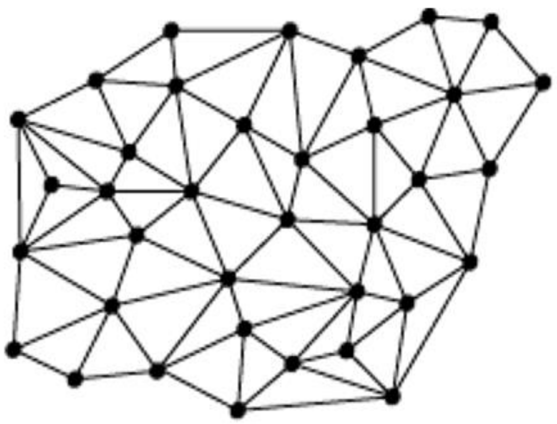


Fig.2.8: Structure of a distributed system

Key features:

1. The system components are concurrent that is it allows systems to be connected to the network at the same time.
2. There will be multiple components, each autonomous in nature.
3. In a distributed system, a global clock is not required. The systems can be spread across multiple geographic locations.
4. When compared with other network models, distributes systems have is greater fault tolerance capability.
5. Price to performance ratio is high

Key goals:

1. *Transparency*

   Achieving the image of a single system without obscuring the details of location, concurrency, relocation, migration, failure, and resources to the handlers.

2. *Openness*

   Making it easy for modification of the network and also to configure it.

3. *Reliability*

   A distributed system should have a high capability of being secure, consistent along with the high capability of masking the errors.

4. *Performance*

   Distributed models are estimated to give a much-wanted improvement to performance.

5. *Scalability*

   Distributed systems should be scalable w.r.t. geography, administration, and size.

Challenges:

1. Security is one of the biggest challenge in a distributed environment, especially when the networks are public.
2. If a distributed system is built using unreliable components, fault tolerance could be challenging.
3. If proper protocols or policies are not used, resource sharing and coordination could be difficult.
4. Process knowledge should be in place so that it would be easy for the administrators and users of the distributed model.

Advantages:

1. A node can share data with other nodes in the network as all the nodes in the distributed system are very well connected to each other.
2. It is scalable according to the requirement (that is more nodes can easily be added whenever required).
3. Node failure does not lead to the failure of the entire system. Other nodes in the network can still communicate with each other.
4. Resources can be shared by multiple nodes rather than just being restricted to one.

Disadvantages:

1. Providing adequate security in distributed systems is difficult as the nodes and the connections need to be secured.
2. Sometimes, while moving from one node to another node in the network, messages, as well as data, could be lost.
3. The database is quite complicated in a distributed system and is difficult to handle when compared to a single user system.
4. Network if all the nodes present in the network of the distributed system try sending data at the same time, overloading may occur.

Blockchains, because of its distributed nature it can be used in a wide range of applications like:

- Land registration (ownership of land).
- Financial services
- Voting
- Digital assets
- Physical assets

Transparency

A system is said to be transparent if the system after a change (like adding a new component or new feature) obeys to the previous interface (external) as much as it can while changing the way it behaves internally. In other words, it is the ability to be easy to see through it.

On blockchain, the user's identity is masked behind dominant cryptography, which means that linking public addresses to different individual users is to achieve particularly. The transparency of a blockchain comes up from the fact that all the transactions of each public address are open to view. It is possible to view the transactions that they have carried out using an explorer along with a user's public address. The level of transparency that blockchain provides to a financial system is relatively very high, especially considering large businesses. It also adds a high degree of accountability. This way the blockchain provides large businesses platform to act with genuine integrity towards their community and customers. Blockchain in addition to financial aspects of the business has the potential to add transparency to other aspects.

Decentralized Application

A DApp is an application that provides a friendly user interface for users of smart contracts. It consists of a front-end interface which includes Browser, HTML, CSS and a back-end interface which is Web3 JS. The application uses JSON RPC to interact with the ethereum node. JSON RPC is a stateless and lightweight RPC which is used by clients to interact with the nodes of ethereum.

Fig 2.8 depicts the structure of DApp.

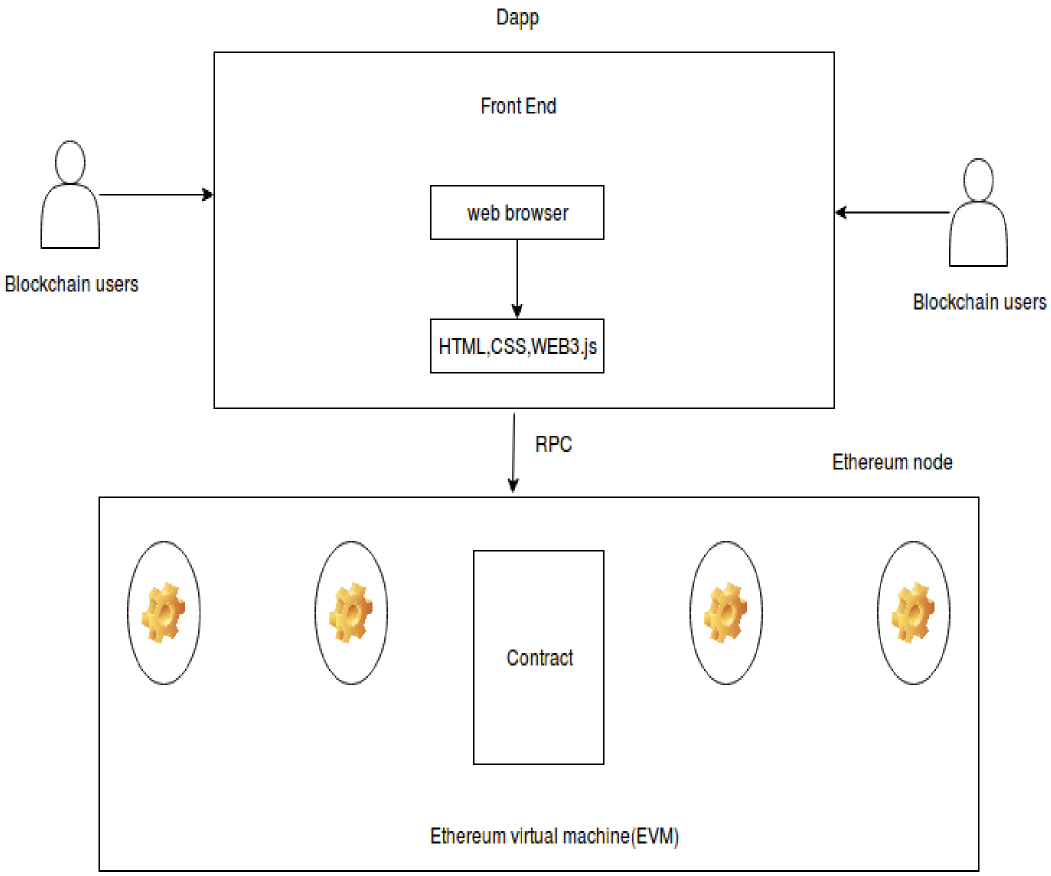


Fig 2.9 DApp structure

Smart contract Structure

A smart contract which is identified by an address in blockchain is a program. Executable functions and state variables are the components of the smart contract. Every transaction has input variables which are mandatory as a function. Depending on the logical implementation, the status of the state parameters are changed. The smart contract programs are written in high-level languages like Python, Solidity. Using compilers such as Solidity or Serpent, the code is compiled into bytecode. Once the code is error-free, the code is uploaded to the network of the blockchain. A unique address will be assigned to each contract by the blockchain network. The functions can be triggered by any legitimate user. Smart contracts that are deployed on a network of blockchain can communicate with other contracts. The components of the message include the sender's address, the receivers address, value of transfer, and a data field which comprises the input data to the receiver's contract. The contract differentiates between transaction and message. A transaction is created by External Owned Account (EOA) while the message is created by a smart contract.

Ethereum is one of the best platforms available for smart contract development. A developer can create formats of transactions, transitions of state, events functions and rules for ownership. Ethereum virtual machine is used for the execution of software code.

Consensus Protocol

Consensus algorithm in the network of blockchain is used to let users agree on the current state of the blockchain even though they do not trust each other and in the absence of a central authority. The most common consensus algorithms are proof of work (PoW), Proof of Stake (PoS). In Proof of work, participating users try to solve difficult mathematical problems, and then give the solutions. It uses resources like computers and electricity to get the solution. The only way to prevent the legitimate users from coming to an agreement about the state of the blockchain is to control enough of the total computing power and pretend that all other users are lying about the state of the blockchain. IN PoS, work will be done regardless of whether someone is trying to interfere or not. In proof of stake, agreement within the blockchain would be measured based on how much digital currency agrees with the current state. Ethereum follows the proof of work but is currently moving to proof of stake. The workflow difference between proof of work and proof of stake is shown in Fig.2.10.

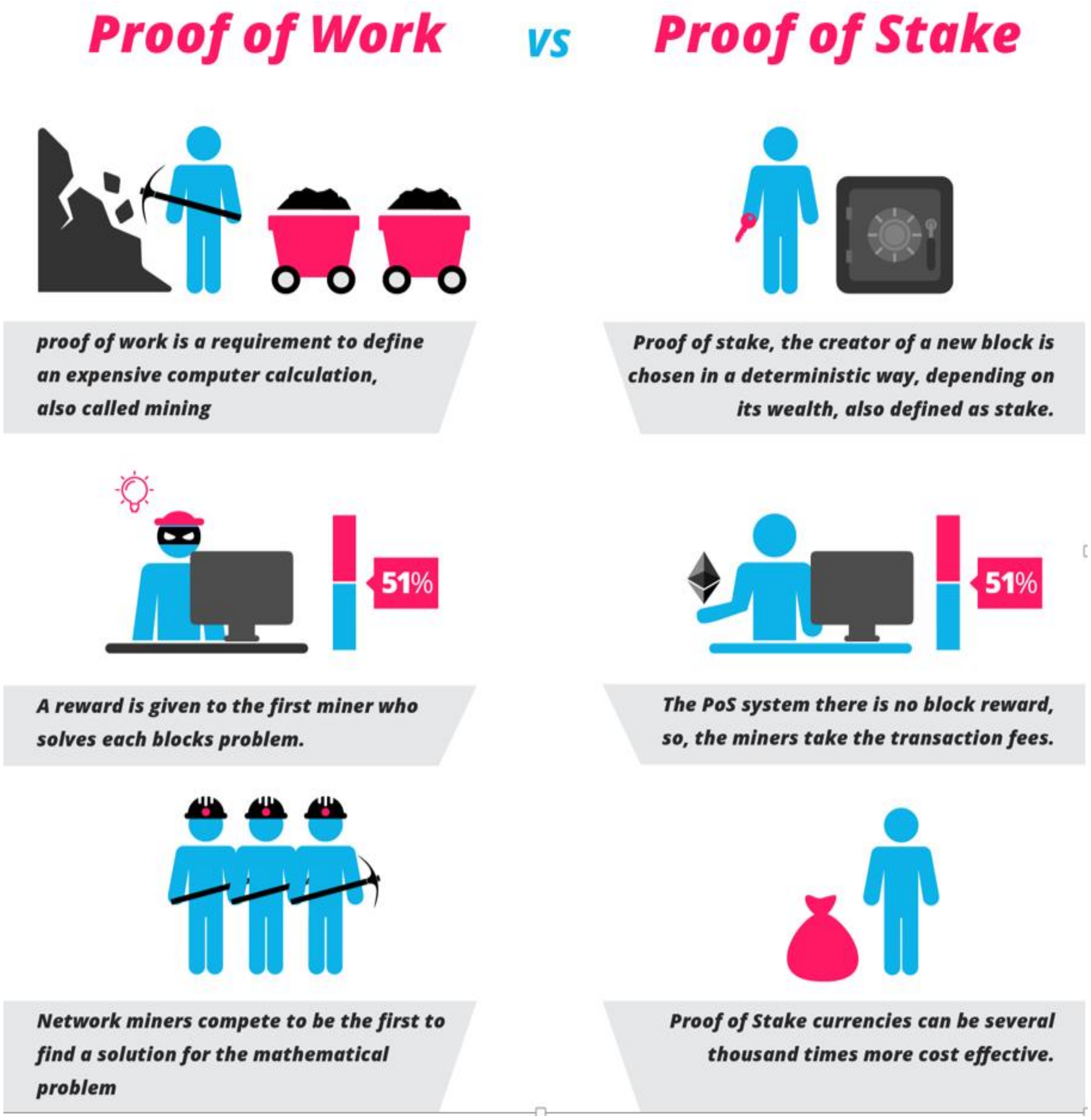

Proof of Work
vs
Proof of Stake
proof of work is a requirement to define an expensive computer calculation, also called mining
Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.
51%
51%
A reward is given to the first miner who solves each blocks problem.
The PoS system there is no block reward, so, the miners take the transaction fees.
Network miners compete to be the first to find a solution for the mathematical problem
Proof of Stake currencies can be several thousand times more cost effective.

Fig.2.10: Proof of work vs Proof of stake

Mining is mainly used for 2 purposes:

1. To verify the validity of a transaction that is to avoid double-spending.
2. To generate new currencies by rewarding the miners for performing the task.

Cryptographic schemes

The process of changing the plain text to cipher text so that it can be passed from one person to another securely is termed as encryption and the process of changing the ciphertext back to its plain text is called decryption. The process is shown in Fig.2.9. These ensure that information is received and processed correctly (that is it provides confidentiality). Momentary keys are used to secure the encryption process. The process by which these keys are generated depends upon the algorithm. Usually, we have a symmetric key and asymmetric key algorithms. The same key is required for encryption and decryption in case of symmetric key algorithms. On the other hand, in asymmetric key or public key algorithms, the pair of keys is used to encrypt and decrypt a message. Few algorithms that provide encryption and decryption are DES, TDES, International Data Encryption Algorithm, Serpent, Blowfish, CAST, RSA (Rivert-Shamir-Adleman), PGP (Pretty Good Privacy), MARS, RC6, TEA, DH, Secure Shell.

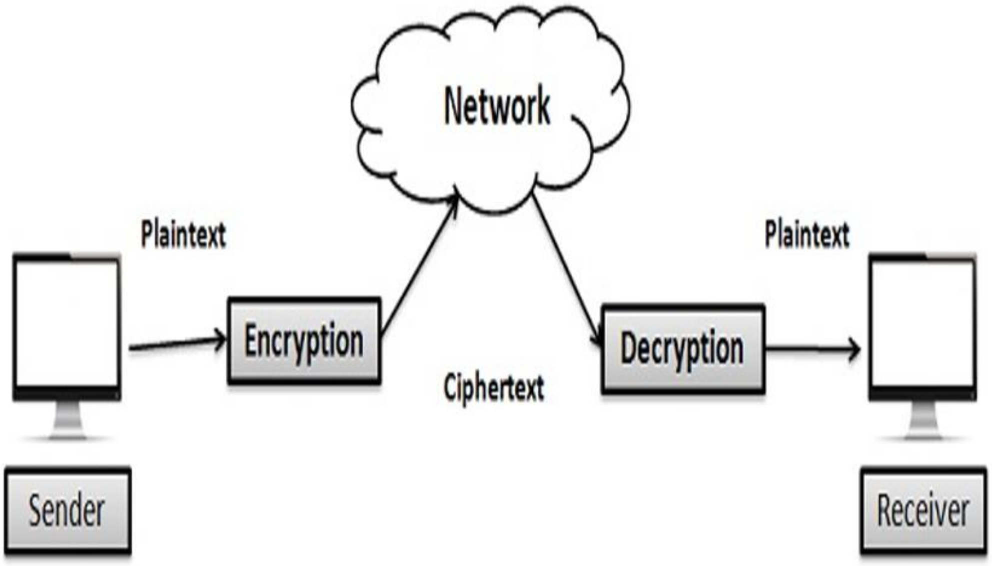


Fig.2.11: Encryption and decryption process

Authentication

Authentication is referred to as a process of identifying a user's identity. It is the mechanism of associating an incoming request with a set of credentials capable of authenticating the sender. The credentials which are provided by the sender are verified using the information available in the local OS or authentication servers that are maintained by key distribution centers (KDC). One way of providing authentication is signing the document or file that is to be sent as shown in Fig.2.10. For data to be communicated over a network, a digital signature is used. It binds an entity to numerical data. The data as well as the signature which are received by the receiver are verified using cryptographic values or secret keys shared between them. Some of the digital signature algorithms are RSA scheme, Digital Signature Algorithm, Elliptical Curve Digital Signature Algorithm, Edwards-curve Digital Signature Algorithm (EdDSA), ElGamal DSS, Hash functions. DSS verify that the integrity of the message has not tampered as well as it is used to guarantee the originators identity. There are many hash algorithms available. Some of them are MD-5, HMAC, SHA-1, SHA-2, and SHA-3. The process of hashing is shown in Fig.2.11

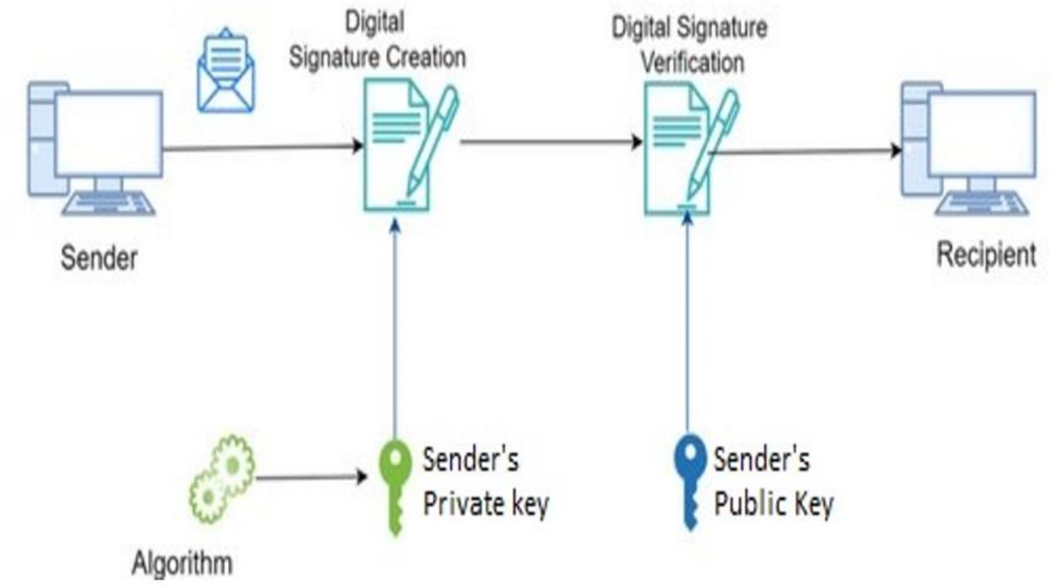


Fig.2.12: Digital Signature Process

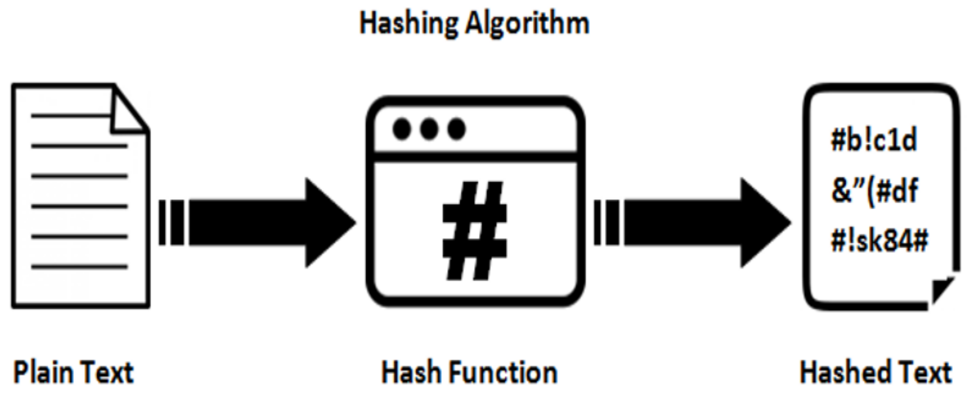


Fig.2.13: Hashing Process

Public key cryptosystem

Public key cryptosystem gained its popularity in signing and encryption operations. As reported on literature, algorithms like RSA, ECC are widely adopted by many real-time applications to enhance security services for users. There are many public key cryptosystems like ElGamal, ECC, and RSA. These algorithms use a key pair which are a public key and private key for the implementation of cryptographic primitives. The algorithms uses 3 phase's for signing namely key generation, signing and verification for authenticating the entity. Literature postulates the wide adoption of DH scheme and variations in it for exchanging secret keys. The strength of the DH scheme is based on the difficulty in solving the discrete log under different fields. RSA algorithm is an asymmetric cryptographic system which is based on the complexity of factorizing long integers which are used to generate the public, private key pairs. Doubling and tripling the key sizes will lead to an increase in the strength of encryption using RSA. In RSA digital signature scheme the private key of the sender is applied to a message to produce a signature. This signature can be verified using the public key to the message and this signature through the verification process gives either a valid or invalid result. The algorithms to guarantee the confidentiality uses three phases which are registration, encryption, and decryption.

Phase 1

1. Generate P and Q randomly.
2. Calculate n as P × Q.
3. Generate E.
4. Compute the value of D,

   $D \equiv E^{-1} \bmod \phi(n)$

At the end of phase 1, the entities that are communicating would have computed the key pairs. The public key is {E, n} and private key is {D}.

Phase 2

Encrypt using public key E,

$$C \equiv M^{E} \bmod n.$$

Phase 3

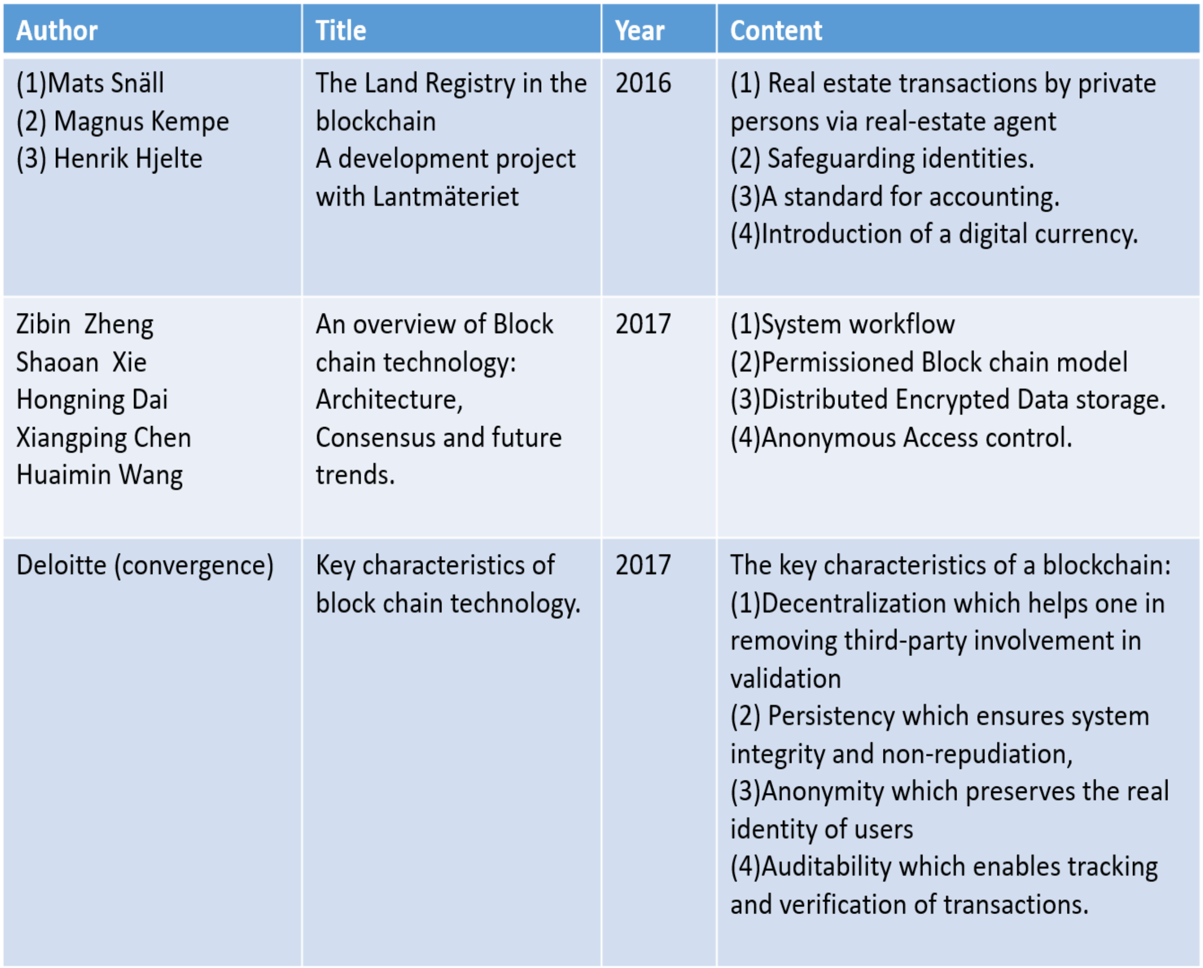
Decrypt using private key D,

$$M \equiv C^{D} \bmod n.$$

Table 2.4: RSA-Notation table

Sno	**Variables**	**Meaning**
1	P	A very large prime number
2	Q	A very large prime number
3	n	The product of 2 large prime numbers
4	E	Public key, $1 \leq E \leq \phi(n) - 1$ and $GCD(E, \phi(n)) = 1$
5	D	Private key
6	M	Plain text/ Message
7	C	Cipher Text

Research papers are undertaken for study



Author	Title	Year	Content
(1)Mats Snäll (2) Magnus Kempe (3) Henrik Hjelte	The Land Registry in the blockchain A development project with Lantmäteriet	2016	(1) Real estate transactions by private persons via real-estate agent (2) Safeguarding identities. (3)A standard for accounting. (4)Introduction of a digital currency.
Zibin Zheng Shaoan Xie Hongning Dai Xiangping Chen Huaimin Wang	An overview of Block chain technology: Architecture, Consensus and future trends.	2017	(1)System workflow (2)Permissioned Block chain model (3)Distributed Encrypted Data storage. (4)Anonymous Access control.
Deloitte (convergence)	Key characteristics of block chain technology.	2017	The key characteristics of a blockchain: (1)Decentralization which helps one in removing third-party involvement in validation (2) Persistency which ensures system integrity and non-repudiation, (3)Anonymity which preserves the real identity of users (4)Auditability which enables tracking and verification of transactions.

Table 2.5: Literature survey summary

CHAPTER 3
SYSTEM SPECIFICATIONS

Software

1. Online Remix IDE

   Remix is an open source tool which enables one to write contracts in Solidity language straight from the browser.

2. IPFS

   IPFS (Inter Planetary File System) stores the files and track accounts over time. When a file is stored in this system it gives a unique hash value. IPFS is a peer to peer distributed file system.

3. Test RPC

   Test RPC is an ethereum client which is used for testing and development. Using ethereumjs it simulates full client behavior which makes developing Ethereum applications much faster. Test RPC gives ten free accounts for testing the codes that are developed.

4. Visual Studio Code

   This is an open source editor used for creating front-end for the applications HTML, CSS, JavaScript codes.

5. Open GPG

   This is used for the purpose of encryption and digital signature. The algorithm used is RSA.

Hardware

1. Laptop

- RAM: 16 GB laptop.
- Processor: Core i7.
- System type: 64-bit Operating system.
- Operating System: Ubuntu (Virtual machine-VMware Workstation pro).
- Graphics: HD-Graphics 520.

Languages

1. Solidity

   The smart contracts developed in online Remix IDE are written in solidity language.

2. HTML

   The front end of the DApp is developed using HTML.

3. JavaScript

   This is used to connect the DApp with the online Remix IDE

4. CSS

   The styling sheets for the front end.

CHAPTER 4
ARCHITECTURE

The proposed system operates as follows:

A buyer and seller — after negotiating the deal of land, has to record their deed through the local authorities. They will proceed to the Government services office as they usually do to register the sale deed. In the Government services office, the systems are now powered by blockchain technology. The admin will encrypt and sign the land documents and store it in IPFS. The IPFS generates a hash which he/she will be using later in the smart contract. He/she will then log in with his/her credentials into the DApp (Decentralized application front end). The authority then checks the validity of land. If the land details are valid, one can proceed to the smart contract page in which he/she enters the details regarding the buyer, seller, change of owner, plot address and other required details along with the hash generated by IPFS. Once the transaction is successful, the block gets created and is added to the blockchain i.e., an automatic transfer of ownership is completed. If the transaction is not successful the admin has to redo the entire process. Figure 4.1 presents the proposed system architecture.

This system which is blockchain enhanced takes the control and records the contract in the presence of buyer and seller. From the manager's viewpoint, there is transparency, efficiency, and accuracy. He /She can observe and keep track of the sale deed and state of the asset in near real-time. In addition, they will have instant access to permanent and complete transaction history regarding each sale and property. The strength of the system is that the citizens who are involved in buying and selling of the property will not require blockchain accounts or blockchain wallets nor will they experience any change in the way they interrelate with the system. The blockchain works quietly and robustly in the background. This procedure will increase civilian's confidence in the government. Most importantly, it will improve the security of data and guarantee the validity of land records.

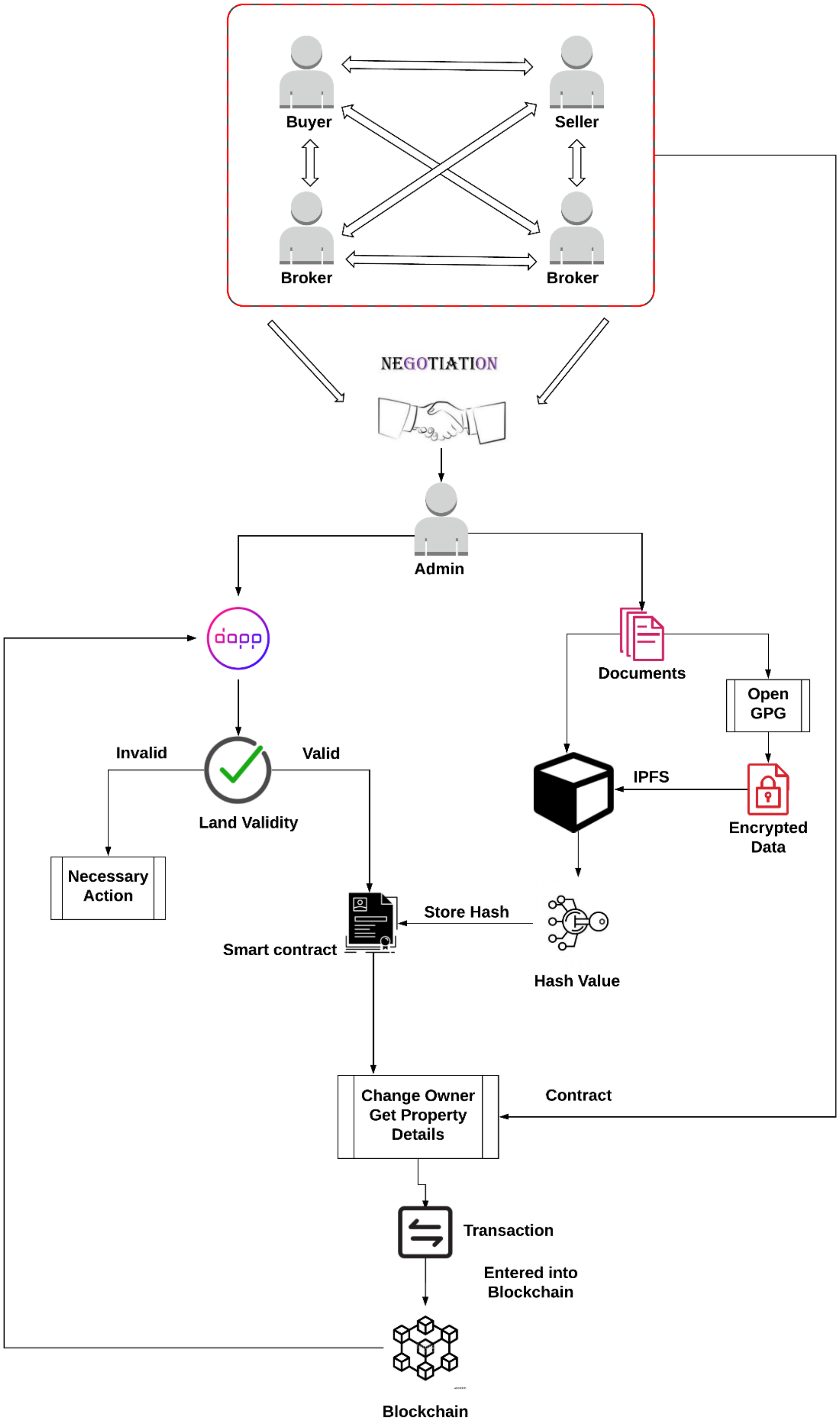
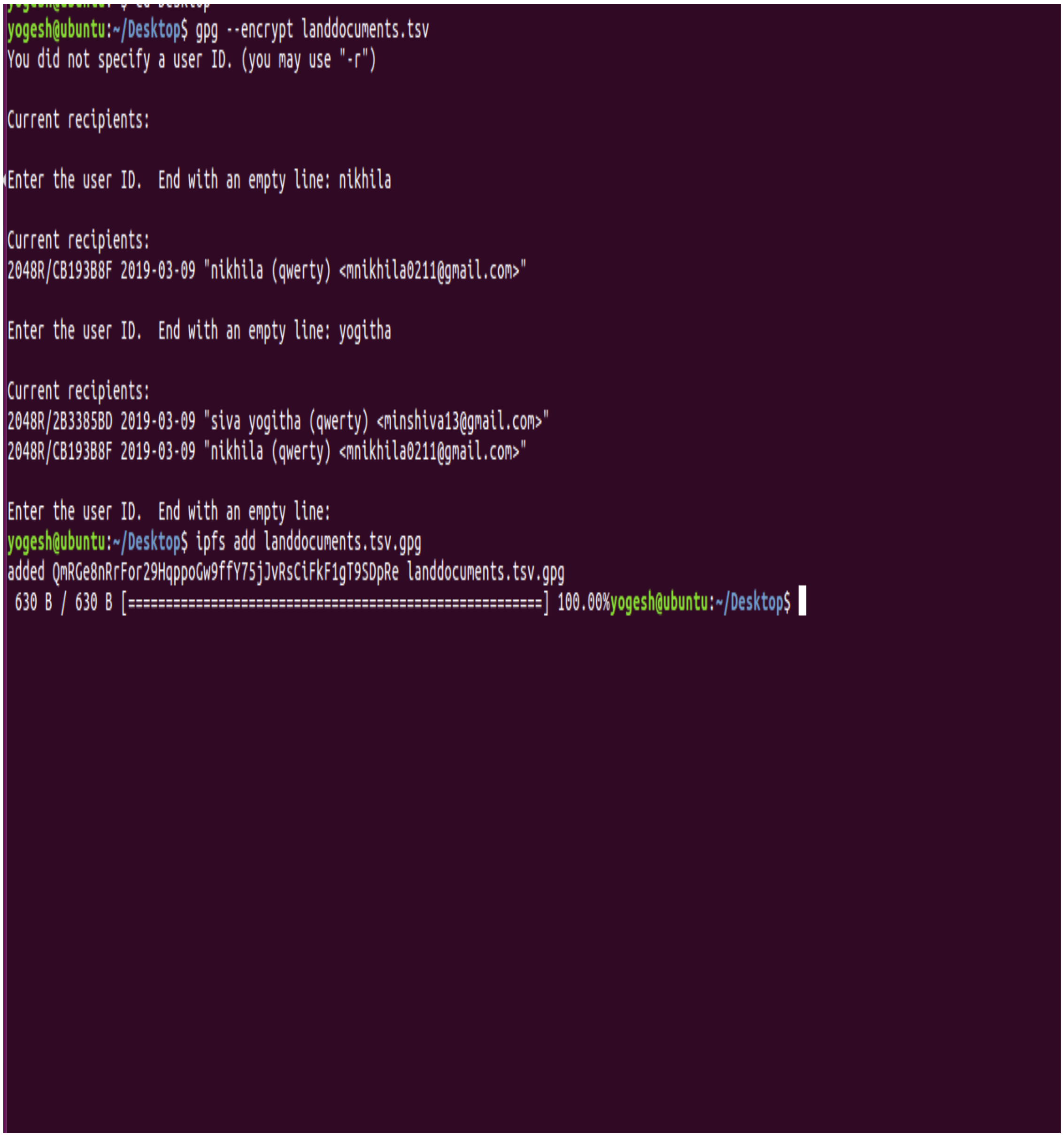


Fig 4.1: Proposed System Architecture

CHAPTER 5
RESULTS AND DISCUSSION

The project uses encryption and digital signature schemes for the purpose of securing land documents and registering transactions in nodes (blocks) of the blockchain. The cryptographic schemes were performed using Open GPG. Considering the strength of RSA, it was chosen as an algorithm for encryption and digital signing of the land registration details. RSA algorithm is an asymmetric cryptographic procedure which is based on the complexity of factorizing long integers that are used to get the public, private key pairs. Doubling and tripling the key sizes leads to an increase in the strength of encryption using RSA. In RSA digital signature scheme the sender's private key is applied to a message to produce a signature. This signature can be verified using the public key to the message and the signature through the verification process, which gives either a valid or invalid result. Keccak256 (SHA 3) is used in smart contracts to map data of random size to data of fixed size. The values that are returned by the hash function are called hash values, hash codes, or simply hashes. It can be used to compare the hash of a document provided by the author, with a calculated hash of a document. As long as they match, it means that the document has not tampered.

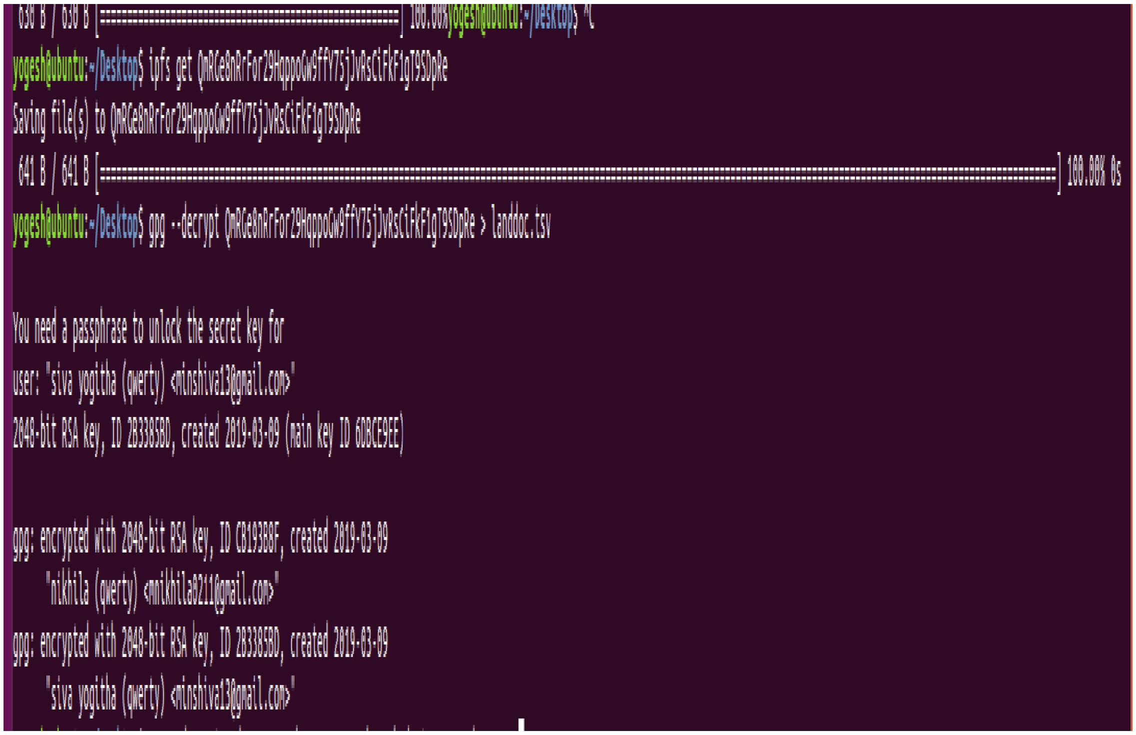
The land documents are encrypted and signed using RSA algorithm by the admin (registrar – a legitimate user who is assigned the task of verifying the entries and initiation of the transaction) at the government office and then saved the land documents in the IPFS. The hash value is returned as shown in Fig.5.1.



```
yogesh@ubuntu:~$ cd Desktop
yogesh@ubuntu:~/Desktop$ gpg --encrypt landdocuments.tsv
You did not specify a user ID. (you may use "-r")

Current recipients:

Enter the user ID.  End with an empty line: nikhila

Current recipients:
2048R/CB193B8F 2019-03-09 "nikhila (qwerty) <mnikhila0211@gmail.com>"

Enter the user ID.  End with an empty line: yogitha

Current recipients:
2048R/2B3385BD 2019-03-09 "siva yogitha (qwerty) <minshiva13@gmail.com>"
2048R/CB193B8F 2019-03-09 "nikhila (qwerty) <mnikhila0211@gmail.com>"

Enter the user ID.  End with an empty line:
yogesh@ubuntu:~/Desktop$ ipfs add landdocuments.tsv.gpg
added QmRGe8nRrFor29HqppoGw9ffY75jJvRsCiFkF1gT9SDpRe landdocuments.tsv.gpg
 630 B / 630 B [=======================================================] 100.00%yogesh@ubuntu:~/Desktop$ 
```

Fig 5.1: Encryption and digital signature using RSA and storing in IPFS

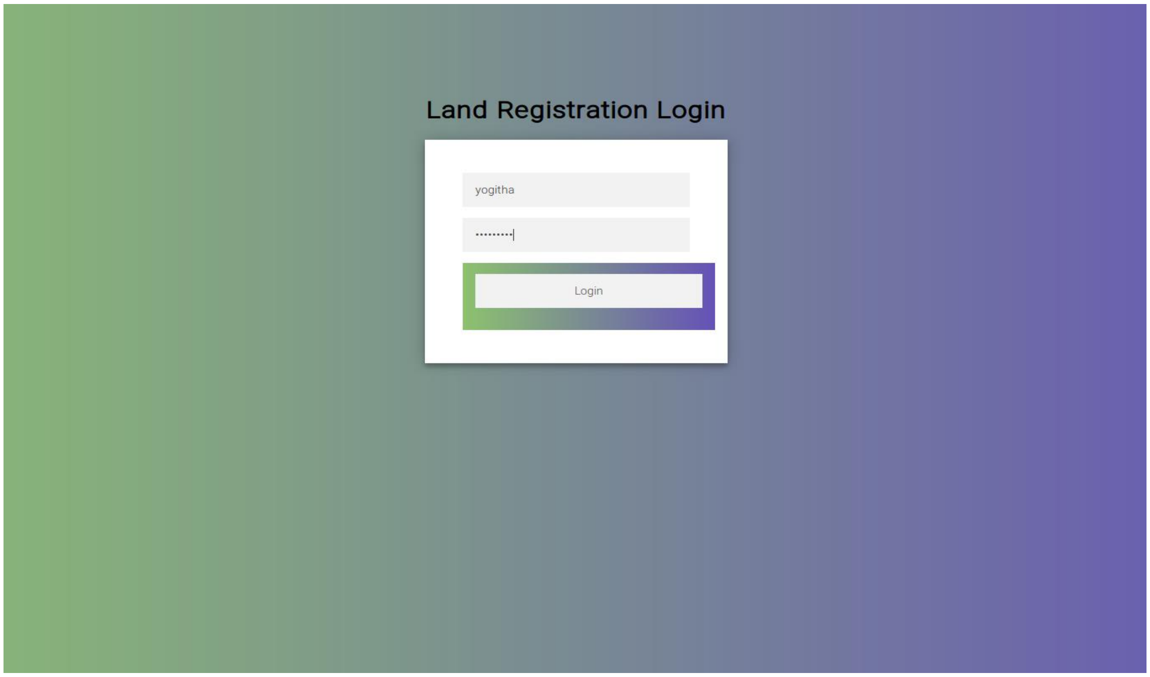
The documents are retrieved from IPFS using the hash and the encrypted file is decrypted to get the original documents as shown in Fig.5.2.



```
 630 B / 630 B [==================================================] 100.00%yogesh@ubuntu:~/Desktop$ ^C
yogesh@ubuntu:~/Desktop$ ipfs get QmRGe8nRrFor29HqppoGw9ffY75jJvRsCiFkF1gT9SDpRe
Saving file(s) to QmRGe8nRrFor29HqppoGw9ffY75jJvRsCiFkF1gT9SDpRe
 641 B / 641 B [==========================================================================================================================================================] 100.00% 0s
yogesh@ubuntu:~/Desktop$ gpg --decrypt QmRGe8nRrFor29HqppoGw9ffY75jJvRsCiFkF1gT9SDpRe > landdoc.tsv


You need a passphrase to unlock the secret key for
user: "siva yogitha (qwerty) <minshiva13@gmail.com>"
2048-bit RSA key, ID 2B3385BD, created 2019-03-09 (main key ID 60BCE9EE)


gpg: encrypted with 2048-bit RSA key, ID CB193B8F, created 2019-03-09
      "nikhila (qwerty) <mnikhila0211@gmail.com>"
gpg: encrypted with 2048-bit RSA key, ID 2B3385BD, created 2019-03-09
      "siva yogitha (qwerty) <minshiva13@gmail.com>"
```

Fig.5.2: Documents retrieved from IPFS and decrypted

The admin (registrar) in the register office logins into the DApp (front end) using his user name and password (private key) to verify the land details as shown in Fig 5.3.



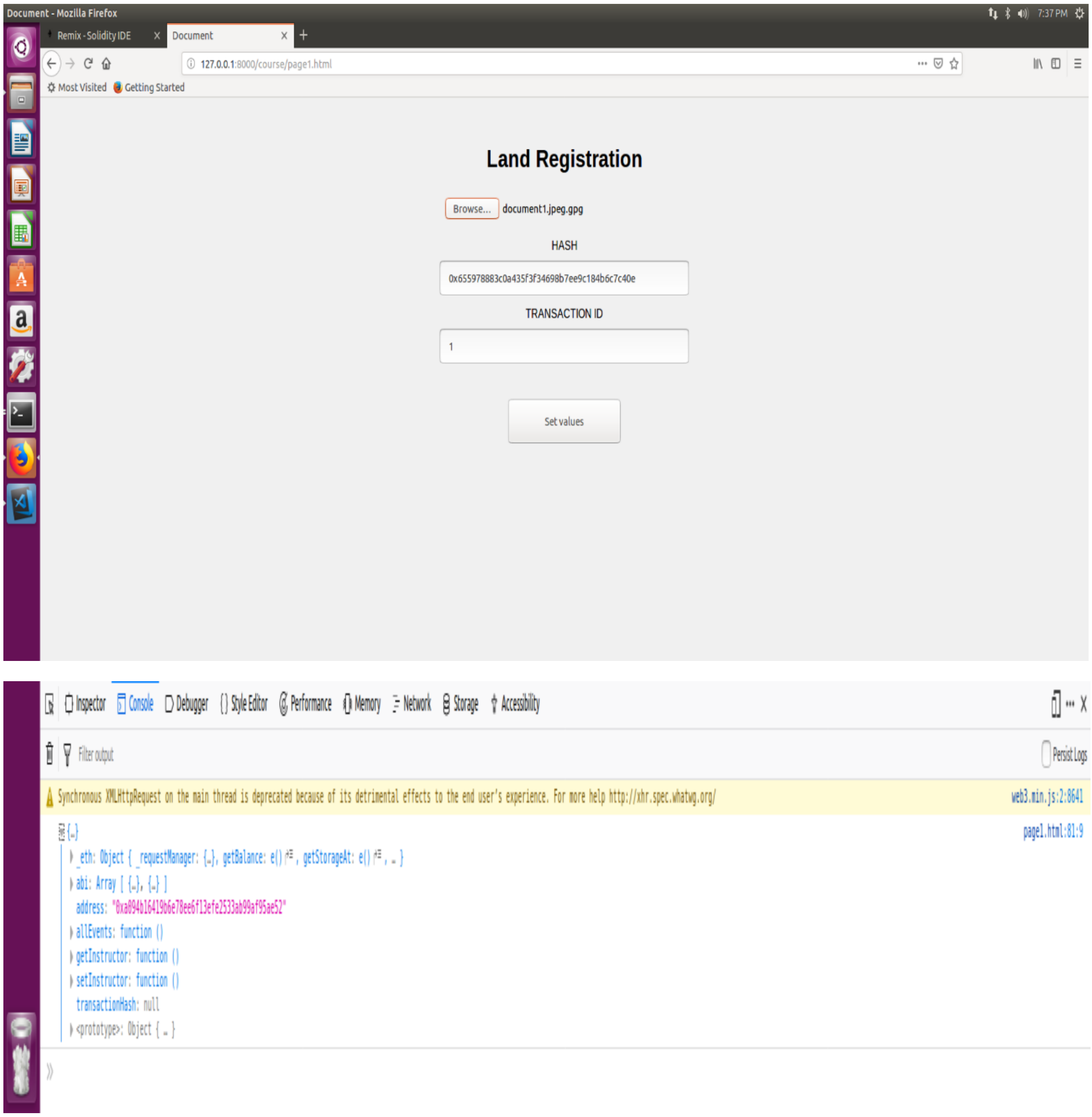
Land Registration Login

yogitha

·········|

Fig.5.3: Login for admin

After the admin logins, he verifies the land details and then makes a transaction giving the plot details and the cost of land that is negotiated. The transaction details appear in the console window as shown in the Fig.5.4.



Land Registration

Browse... document1.jpeg.gpg

HASH

0x655978883c0a435f3f34698b7ee9c184b6c7c40e

TRANSACTION ID

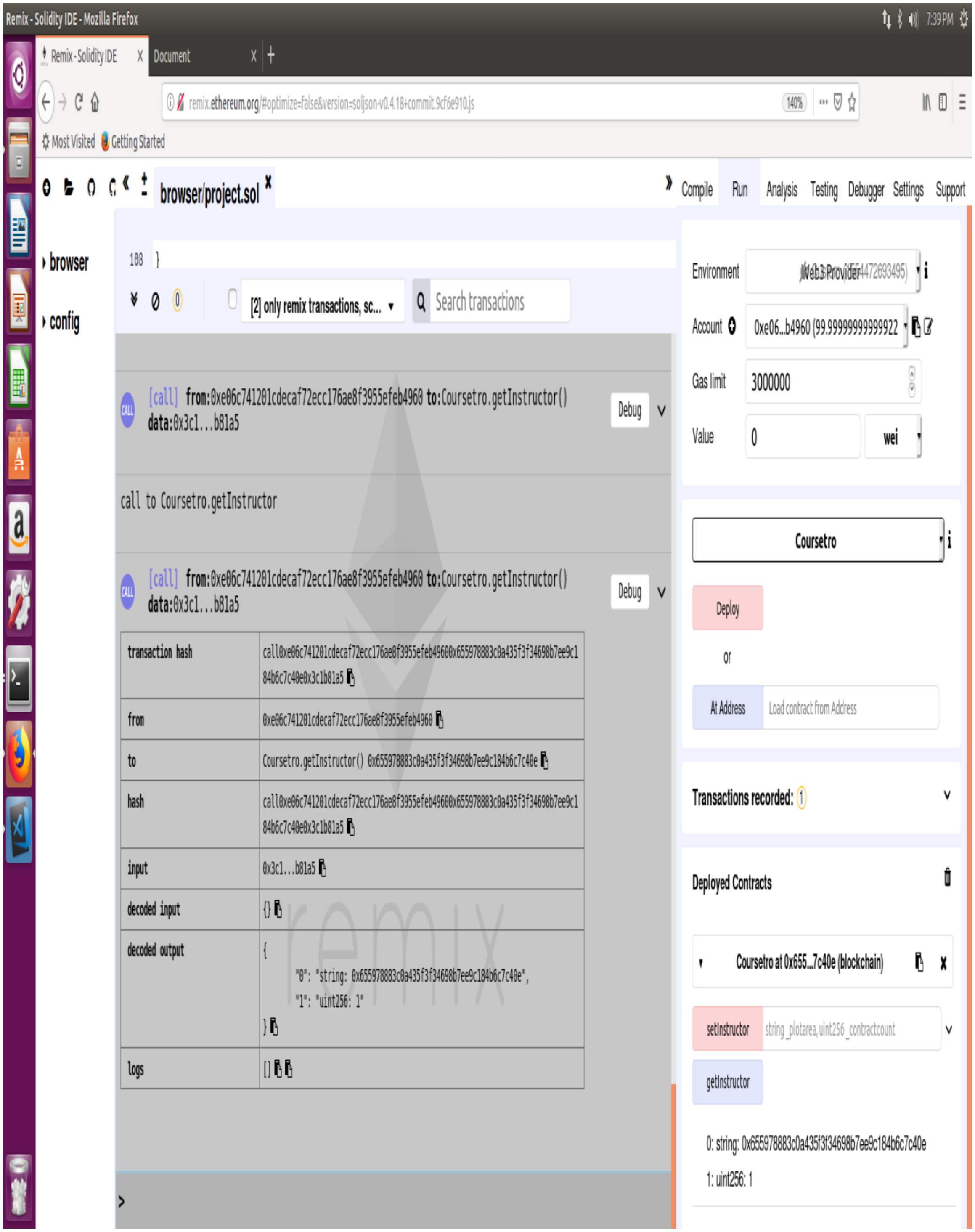
1

Set values

```
Synchronous XMLHttpRequest on the main thread is deprecated because of its detrimental effects to the end user's experience. For more help http://xhr.spec.whatwg.org/    web3.min.js:2:8641
{…}                                                                                   page1.html:81:9
  _eth: Object { _requestManager: {…}, getBalance: e(), getStorageAt: e(), … }
  abi: Array [ {…}, {…} ]
  address: "0xa094b16419b6e78ee6f13efe2533ab99af95ae52"
  allEvents: function ()
  getInstructor: function ()
  setInstructor: function ()
  transactionHash: null
  <prototype>: Object { … }
```

Fig.5.4: The land details are taken from the front end

The values from the front end are retrieved at the back end and the details are shown in the transaction. Fig 5.5 depicts this.



```
108 }

[call] from:0xe06c741201cdecaf72ecc176ae8f3955efeb4960 to:Coursetro.getInstructor()
data:0x3c1...b81a5

call to Coursetro.getInstructor

[call] from:0xe06c741201cdecaf72ecc176ae8f3955efeb4960 to:Coursetro.getInstructor()
data:0x3c1...b81a5
```

transaction hash	call0xe06c741201cdecaf72ecc176ae8f3955efeb49600x655978883c0a435f3f34698b7ee9c184b6c7c40e0x3c1b81a5
from	0xe06c741201cdecaf72ecc176ae8f3955efeb4960
to	Coursetro.getInstructor() 0x655978883c0a435f3f34698b7ee9c184b6c7c40e
hash	call0xe06c741201cdecaf72ecc176ae8f3955efeb49600x655978883c0a435f3f34698b7ee9c184b6c7c40e0x3c1b81a5
input	0x3c1...b81a5
decoded input	{}

decoded output	{
	"0": "string: 0x655978883c0a435f3f34698b7ee9c184b6c7c40e",
	"1": "uint256: 1"
	}

logs	[]

Environment Web3 Provider

Account 0xe06...b4960 (99.99999999999922

Gas limit 3000000

Value 0 wei

Coursetro

Transactions recorded: 1

Deployed Contracts

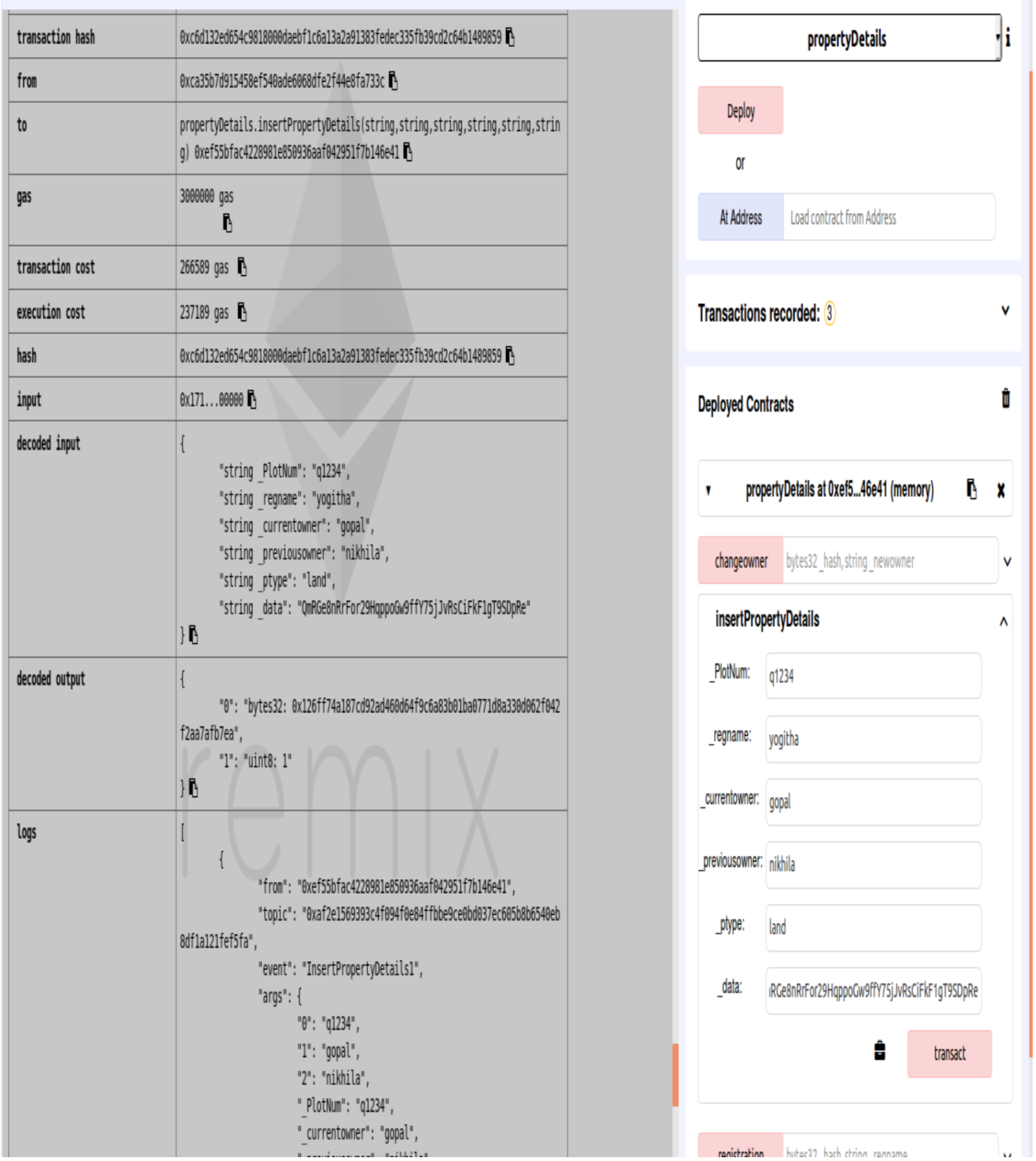
Coursetro at 0x655...7c40e (blockchain)

0: string: 0x655978883c0a435f3f34698b7ee9c184b6c7c40e

1: uint256: 1

Fig 5.5: Transaction depicting values from the front end

Fig 5.6 shows that the function insert property details takes the registrar name, sellers name, buyers name, land details and the hash value of documents taken from the IPFS and return the status of the transaction. This status is byte 32 value which is unique for the transaction. We can get the details of the transaction using this value.



transaction hash	0xc6d132ed654c9818000daebf1c6a13a2a91383fedec335fb39cd2c64b1489859
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	propertyDetails.insertPropertyDetails(string,string,string,string,string,string) 0xef55bfac4228981e850936aaf042951f7b146e41
gas	3000000 gas
transaction cost	266589 gas
execution cost	237189 gas
hash	0xc6d132ed654c9818000daebf1c6a13a2a91383fedec335fb39cd2c64b1489859
input	0x171...00000

decoded input	{
	"string _PlotNum": "q1234",
	"string _regname": "yogitha",
	"string _currentowner": "gopal",
	"string _previousowner": "nikhila",
	"string _ptype": "land",
	"string _data": "QmRGe8nRrFor29HqppoGw9ffY75jJvRsCiFkF1gT9SDpRe"
	}

decoded output	{
	"0": "bytes32: 0x126ff74a187cd92ad460d64f9c6a83b01ba0771d8a330d062f042f2aa7afb7ea",
	"1": "uint8: 1"
	}

logs	[
	{
	"from": "0xef55bfac4228981e850936aaf042951f7b146e41",
	"topic": "0xaf2e1569393c4f094f0e84ffbbe9ce0bd037ec605b8b6540eb8df1a121fef5fa",
	"event": "InsertPropertyDetails1",
	"args": {
	"0": "q1234",
	"1": "gopal",
	"2": "nikhila",
	"_PlotNum": "q1234",
	"_currentowner": "gopal",
	"_previousowner": "nikhila"

propertyDetails
Deploy
or
At Address
Load contract from Address
Transactions recorded: 3
Deployed Contracts
propertyDetails at 0xef5...46e41 (memory)
changeowner
bytes32 _hash, string _newowner
insertPropertyDetails
transact
registration
bytes32 _hash, string _regname

_PlotNum: q1234

_regname: yogitha

_currentowner: gopal

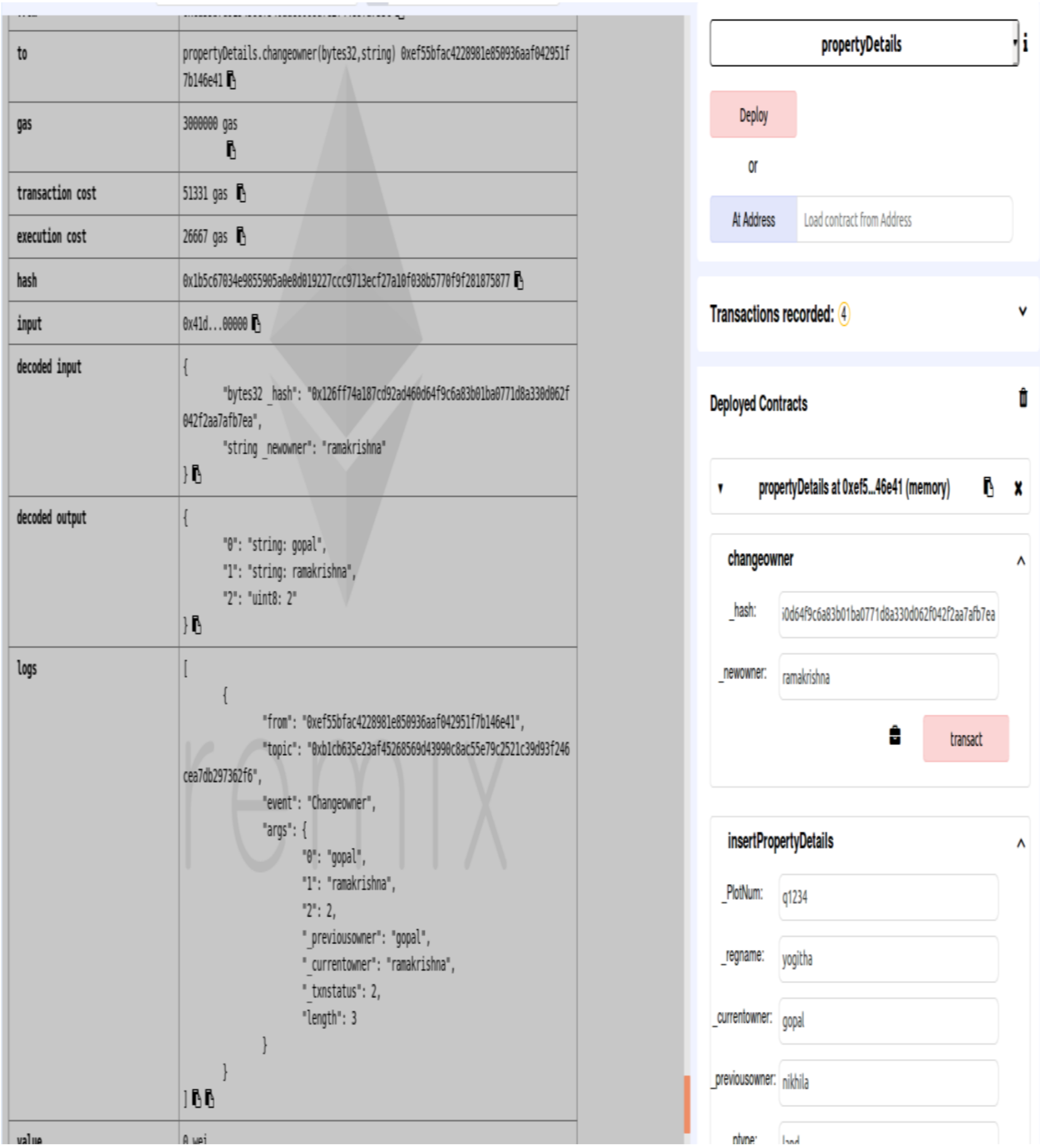
_previousowner: nikhila

_ptype: land

_data: iRGe8nRrFor29HqppoGw9ffY75jJvRsCiFkF1gT9SDpRe

Fig.5.6: Insert property details function and transaction

If the owner of the land wants to sell his land to someone else, he can register it using the change owner function also. But for that, he needs to know the status value (byte 32 value) of the previous transaction, as shown in Fig 5.7.



```
to                 propertyDetails.changeowner(bytes32,string) 0xef55bfac4228981e850936aaf042951f
                   7b146e41
gas                3000000 gas
transaction cost   51331 gas
execution cost     26667 gas
hash               0x1b5c67034e9855905a0e8d019227ccc9713ecf27a10f038b5770f9f281875877
input              0x41d...00000
decoded input      {
                        "bytes32 _hash": "0x126ff74a187cd92ad460d64f9c6a83b01ba0771d8a330d062f
                   042f2aa7afb7ea",
                        "string _newowner": "ramakrishna"
                   }
decoded output     {
                        "0": "string: gopal",
                        "1": "string: ramakrishna",
                        "2": "uint8: 2"
                   }
logs               [
                        {
                             "from": "0xef55bfac4228981e850936aaf042951f7b146e41",
                             "topic": "0xb1cb635e23af45268569d43990c8ac55e79c2521c39d93f246
                   cea7db297362f6",
                             "event": "Changeowner",
                             "args": {
                                  "0": "gopal",
                                  "1": "ramakrishna",
                                  "2": 2,
                                  "_previousowner": "gopal",
                                  "_currentowner": "ramakrishna",
                                  "_txnstatus": 2,
                                  "length": 3
                             }
                        }
                   ]
value              0 wei
```

propertyDetails

Transactions recorded: 4

Deployed Contracts

propertyDetails at 0xef5...46e41 (memory)

changeowner

_hash: i0d64f9c6a83b01ba0771d8a330d062f042f2aa7afb7ea

_newowner: ramakrishna

insertPropertyDetails

_PlotNum: q1234

_regname: yogitha

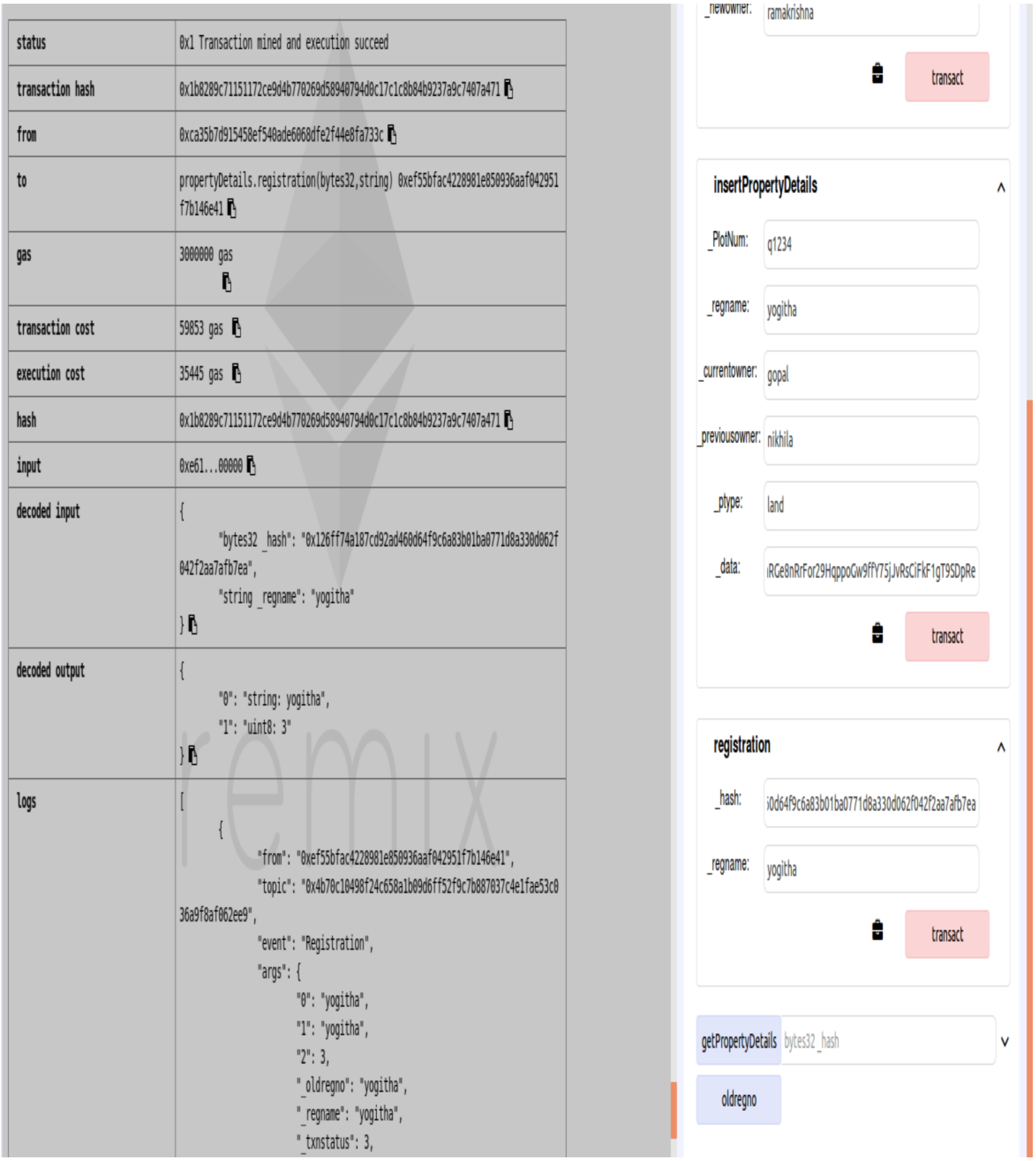
_currentowner: gopal

_previousowner: nikhila

ptype: land

Fig 5.7: Change owner function and transaction

The registrar's details will also be recorded using the byte 32 value as shown in Fig.5.8.



```
status            0x1 Transaction mined and execution succeed
transaction hash  0x1b8289c71151172ce9d4b770269d58940794d0c17c1c8b84b9237a9c7407a471
from              0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to                propertyDetails.registration(bytes32,string) 0xef55bfac4228981e850936aaf042951
                  f7b146e41
gas               3000000 gas
transaction cost  59853 gas
execution cost    35445 gas
hash              0x1b8289c71151172ce9d4b770269d58940794d0c17c1c8b84b9237a9c7407a471
input             0xe61...00000
decoded input     {
                        "bytes32 _hash": "0x126ff74a187cd92ad460d64f9c6a83b01ba0771d8a330d062f
                  042f2aa7afb7ea",
                        "string _regname": "yogitha"
                  }
decoded output    {
                        "0": "string: yogitha",
                        "1": "uint8: 3"
                  }
logs              [
                        {
                              "from": "0xef55bfac4228981e850936aaf042951f7b146e41",
                              "topic": "0x4b70c10498f24c658a1b09d6ff52f9c7b887037c4e1fae53c0
                  36a9f8af062ee9",
                              "event": "Registration",
                              "args": {
                                    "0": "yogitha",
                                    "1": "yogitha",
                                    "2": 3,
                                    "_oldregno": "yogitha",
                                    "_regname": "yogitha",
                                    "_txnstatus": 3,
```

_newowner: ramakrishna

insertPropertyDetails

_PlotNum: q1234

_regname: yogitha

_currentowner: gopal

_previousowner: nikhila

_ptype: land

_data: iRGe8nRrFor29HqppoGw9ffY75jJvRsCiFkF1gT9SDpRe

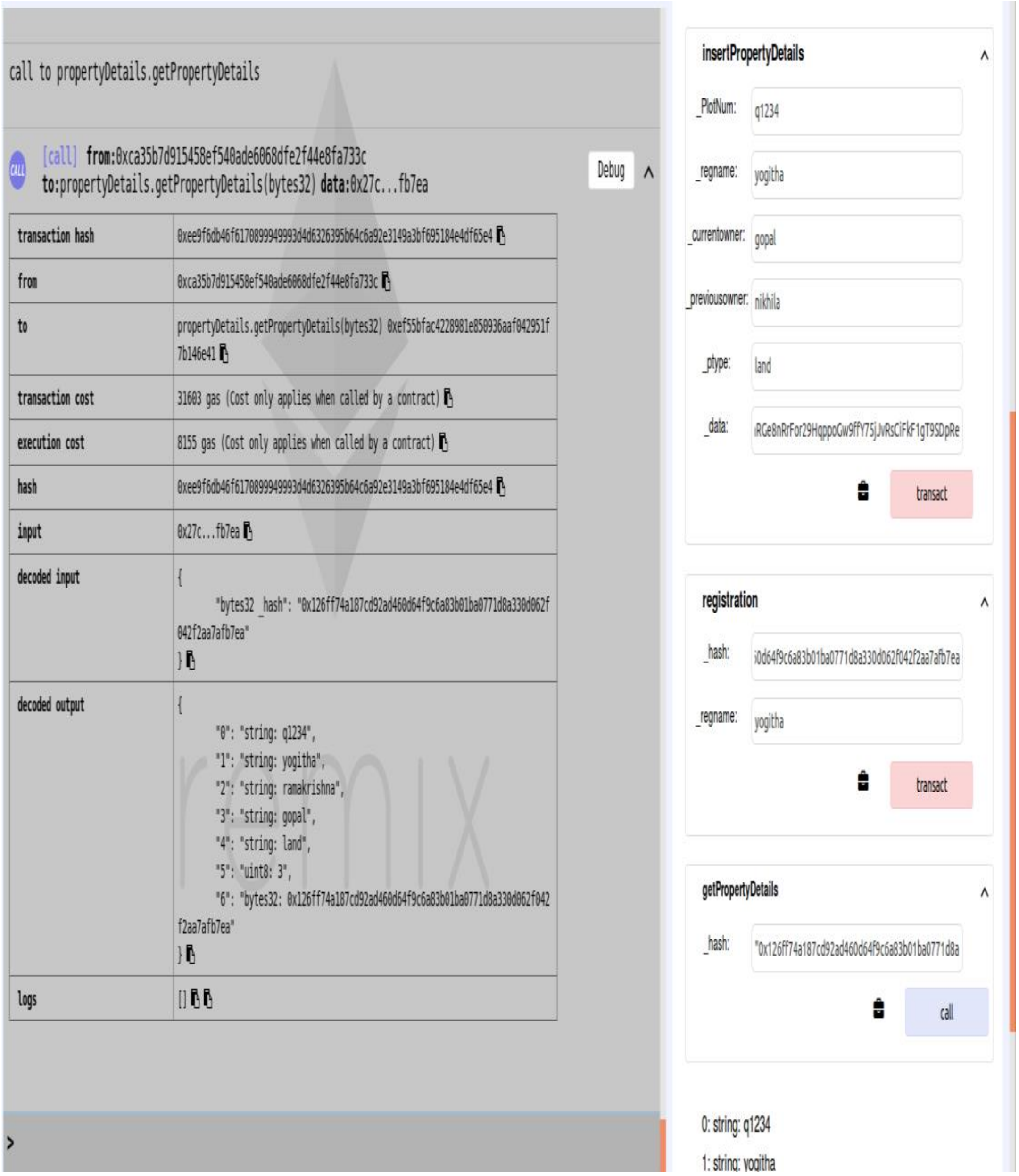
registration

_hash: i0d64f9c6a83b01ba0771d8a330d062f042f2aa7afb7ea

_regname: yogitha

Fig.5.8: Registration function and transaction

The property details can be retrieved by making a call to get property details as shown in Fig.5.9.



call to propertyDetails.getPropertyDetails

[call] **from:**0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to:propertyDetails.getPropertyDetails(bytes32) **data:**0x27c...fb7ea

transaction hash	0xee9f6db46f6170899949993d4d6326395b64c6a92e3149a3bf695184e4df65e4
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	propertyDetails.getPropertyDetails(bytes32) 0xef55bfac4228981e850936aaf042951f7b146e41
transaction cost	31603 gas (Cost only applies when called by a contract)
execution cost	8155 gas (Cost only applies when called by a contract)
hash	0xee9f6db46f6170899949993d4d6326395b64c6a92e3149a3bf695184e4df65e4
input	0x27c...fb7ea

decoded input	{
	"bytes32 _hash": "0x126ff74a187cd92ad460d64f9c6a83b01ba0771d8a330d062f042f2aa7afb7ea"
	}

decoded output	{
	"0": "string: q1234",
	"1": "string: yogitha",
	"2": "string: ramakrishna",
	"3": "string: gopal",
	"4": "string: land",
	"5": "uint8: 3",
	"6": "bytes32: 0x126ff74a187cd92ad460d64f9c6a83b01ba0771d8a330d062f042f2aa7afb7ea"
	}

logs	[]

insertPropertyDetails

_PlotNum: q1234

_regname: yogitha

_currentowner: gopal

_previousowner: nikhila

_ptype: land

_data: iRGe8nRrFor29HqppoGw9ffY75jJvRsCiFkF1gT9SDpRe

registration

_hash: i0d64f9c6a83b01ba0771d8a330d062f042f2aa7afb7ea

_regname: yogitha

getPropertyDetails

_hash: "0x126ff74a187cd92ad460d64f9c6a83b01ba0771d8a

0: string: q1234

1: string: yogitha

Fig.5.9: Get property details function

CHAPTER 6
CONCLUSION

Blockchain with its key characteristics- decentralization, anonymity, persistence, and auditability has shown its potential for transforming the traditional industry. It offers security along with transparency. Using blockchain most of the principles concerning good governance in land administration can be met. In the present land registration systems, the validity of the transactions is mostly done by hand, by scrutinizing the deed. The business rules incorporated in the stylesheet can be relatively similar to the transaction rules in the smart contract that can be used in the blockchain technology. Therefore, one may conclude that in case a Registrar is planning to introduce automated processing of deeds, blockchain could be one of the possibilities. However, to ensure that this is possible, furthermore research is required. Governments are working with this technology to reap the benefits it provides, which were not possible a decade ago. If successful, blockchain, with all its promised benefits, could be that silver bullet solution to cure India's land records administration woes. The future scope for this project includes – Sending confirmation messages to the buyer and seller as well as digitalizing the verification of land records. In conclusion, "The blockchain is not going to 'replace government' concerning how land is registered and monitored. It will make governance of land registration the simplest and most corruption resistant possible". It is not a cure but, is the best tool to fight corruption and inefficacy.

REFERENCES

1) Sarah Underwood, "*Blockchain Beyond Bitcoin*", Communications of the ACM, vol. 59, no. 11, pp. 15-17, November 2016.
2) Don Tapscott and Alex Tapscott, "*Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money,Business, and the World", 1st ed. New York*, USA: Penguin Publishing Group, 2016.
3) Aljosha Judmayer, Nicholas Stifter, Katharina Krombholz, Edgar Weippl, Elisa Bertino, Ravi Sandhu, "*Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms*", IEEE 2017.
4) Y. Zhu and Z. Chen, "RealID: *Building a Secure Anonymous yet Transparent Immutable ID Service*", IEEE 2017.
5) Zheng, Zibin, Xie, Shaoan, Dai, Hong-Ning,Chen, Xiangping, Wang, Huaimin, "*An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*", IEEE 2017.
6) K. Manivannan and D. Academics, "*Contribution of blockchain technology to the growth of the society*", IEEE 2018.
7) S. A. Kalamsyah, A. M. Barmawi and M. Arzaki, "*Digital Contract Using Block Chaining and Elliptic Curve Based Digital Signature*", IEEE 2018.
8) Mahdi H. Miraz and Maaruf Ali, "*Blockchain Enabled Enhanced IoT Ecosystem Security*", 2017, in proceedings of the First International Conference on Emerging Technologies in Computing 2018 (iCETiC '18), London, UK, 23 August 2018.
9) Mahdi H. Miraz and Maaruf Ali, "*Applications of block chain beyond Cryptocurrency*", AETiC 2018.
10) Mahdi H.Miraz, David C.Donald, *"Application of Blockchain in booking and registration systems of security exchanges",* IEEE 2018.
11) M. Memon, U. A. Bajwa, A. Ikhlas, Y. Memon, S. Memon and M. Malani, "*Blockchain Beyond Bitcoin: Block Maturity Level Consensus Protocol*", 2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS), 2018.

12) J Ahmed, A Bhulia, RA Ahmed, AM Hossain*, “An in depth exploration on Blockchain technology using Cryptocurrency”,* 2019.

13) John Adler; Ryan Berryhill; Andreas Veneris; Zissis Poulos; Neil Veira; Anastasia Kastania, *“A Decentralized Blockchain Oracle”,*2018.

14) Vincent Chia, Pieter H. Hartel, Qingze Hum, Sebastian Ma, Georgios Piliouras, Daniel Reijsbergen, Mark van Staalduinen, Pawel Szalachowski, *“Rethinking Blockchain Security: Position Paper”,* 2018.

15) Fthi Abadi, Joshua Ellul, George Azzopardi*,”The Blockchain of Things, Beyond Bitcoin: A Systematic Review”,* 2018.

16) Quinten Stokkink, Johan Pouwelse*,”Deployment of a Blockchain-Based Self-Sovereign Identity”,* 2018.

17) Supriya Thakur Aras,Vrushali Kulkarni*,”Blockchain and its applications-A detailed survey”,* 2017.

18) Michael crosby, Nachiappan, Pradhan pattanayak, Sanjeev verma,Vignesh kalyanaraman*, “Blockchain technology beyond bitcoin”,* 2015.

19) Rishav Chatterjee, Rajdeep Chatterjee*,”An overview of emerging technology: Blockchain*”,IEEE 2017.

20) Harry halpin, Marta piekarska*,”Introduction to security and privacy on the Blockchain”,* IEEE 2017.

21) Sachichanand singh, Nirmala singh,”*Blockchain: Future of cyber security”,* IEEE 2017.

22) Weizhi Meng, Zheng Yan,*”Symposium on Recent Advances on Blockchain and Its Applications (BlockchainApp)”*, IEEE.2017

23) Laurence T. Yang, Zheng Yan,”*International conference on Blockchain*”, IEEE 2018.