Webology (ISSN: 1735-188X)
Volume 19, Number 2, 2022

Blockchain Technology For Improving Land Registration System In An Emerging Economy

Pedro Neves Mata[1] ; Muhammad Najib Razali*[2] , Rui Miguel Dantas[3] ; Mário Nuno Mata[4] , Rohaya Abdul Jalil[5] , José Moleiro Martins[6] , AinurZaireen Zainuddin[7] ; Norhidayah Mohd Yunos[8]

1 Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR-IUL, Lisboa, Portugal.

2 Universiti Teknologi Malaysia.

3 ISCAL-Instituto Superior de Contabilidade e Administração de Lisboa, Instituto Politécnico de Lisboa, Avenida Miguel Bombarda 20, 1069-035 Lisboa.

[4]ISCAL-Instituto Superior de Contabilidade e Administração de Lisboa, Instituto Politécnico de Lisboa, Avenida Miguel Bombarda 20, 1069-035 Lisboa.

[5]UniversitiTeknologi Malaysia;

[6]ISCAL-Instituto Superior de Contabilidade e Administração de Lisboa, Instituto Politécnico de Lisboa, Avenida Miguel Bombarda 20, 1069-035 Lisboa, Portugal.

[7]Universiti Teknologi Malaysia.

[8]Universiti Teknologi Malaysia.

Abstract: Land registration requires complex sensitive data which requires a decentralised environment. Current technology only concentrates on the database storage which is less secure and can be exposed to any misconduct. This is due to the characteristics of the database having problems with unstructured data and non-relational databases. Fraud is one the major problems and is currently a serious problem within the Malaysian land registration system. The blockchain technology creates public ledgers from all complex transactions that have high potential to replace the complicated systems with one simple database. Current practice at the land office has seen the land registration process being very centralised which requires only several persons to validate and authorise the data. Therefore, the need to identify the model of the blockchain technology for land registration is essential. In addition, the foundation of the blockchain technology for the land registration system in Malaysia should be undertaken.

Keywords: Technology, Blockchain, Land, Registration, Malaysia

1. Introduction

Land registration requires complex sensitive data which requires a decentralised environment. According to Vos (2016), the common pattern for land registration consists of object (spatial unit), right (personal rights) and subject (title holder of the right which is related to the subject). As a land registration system requires complexities and challenges in terms of land tenure security on a high-risk scale, the security level of a land registration system needs to be put at the highest level. Fraud is one the major problems, as well as long processing problems. This is due to the centralised transaction system, which results in bottlenecks at the processing system. The blockchain technology creates public ledgers from all complex transactions and has high potential to replace the complicated systems with one simple database. Consequently, the security system will be easier to be managed. In addition, it can be seen that blockchain technology has great potential for the land registration process for the fundamental aspects; especially in terms of technical challenges needing to be addressed. Furthermore, research on the land registration process has been less explored, which resulted in the land registration process being a very slow process. The slow process in land registration is due to several problems including land title registration's serial numbers to the parcels of land, location, boundaries and other land details such a freehold, leasehold, period of years, caveats, easements and encumbrances. Therefore, this paper is aimed to identify characteristics of blockchain technology for land registrations in Malaysia.

The land registration process is a series of complex operations of sharing and processing sensitive data that requires a decentralised environment. The characteristic of land rights are a complicated element, especially when the rights of the land have been manipulated. Therefore, the validation process plays a major role in the land administration process. According to research by Hoxha and Sadiku (2019), even with technological advancements, the real estate transaction system is slow due to validation based on papers. Also, the land registration process faces long processing problems. Furthermore, current technology only concentrates on less secure database storage and can be exposed to any misconduct. As the land registration methods require complexities and challenges in terms of land tenure security at a high-risk scale, the land registration system's security level needs to be put at the highest level. The lack of effectiveness will lead to numerous transparency problems, higher transaction costs, processing delays and personal prejudices (Shiller 2005). Fraud is one of the major problems and is a severe problem for land registration methods. The land title is the confirmation that the land is already registered and includes the owner of the land. The reason for ownership is to perceive property rights, which incorporates data relating to land region, area, limits, just as a proprietorship, and title of the ardent property. However, the land is registered, but there are many causes of fraud in which land registration data can be quickly deleted and or edited. Since land is an asset, and any fraud can cause huge monetary losses, it is crucial that the registration of land becomes speedy, transparent, and with less fraud. In this research, a framework for secure data storage of land registration using blockchain technology is proposed. Blockchain offers a solution with its underlying technology. Blockchain is decentralised, transparent, and fast compared to the traditional centralised software approach. For the validation of the proposed framework, a comparison is performed between proposed and existing methods. All these inefficiencies of real estate transactions, including the land registration system, can be improved through blockchain technology.

2. Literature Review

The common problems in the land registration system involve three elements, and they are spatial unit, personal rights and title holder. These elements all contain information regarding the land registration system. The huge volume of information in these elements creates data complexities when combined with different rights. Land governance is generally considered as the rules, processes and structures through which decisions are made about access to land and its use, the manner in which the decisions are implemented and enforced and the way that competing interest in land is managed (Palmer et al. 2009). Therefore, the land registration process needs to have important characteristics such as data creation, data management and data usage. These characteristics need to have high security and be protected by high encryption. Land tenure security is sought after, studied and measured in different ways by different disciplinary domains and industry sectors (Simbizi et al. 2014). The high-level security of a land registration system will also create stable governance and institutions. According to Williamson et al. (2010) ingredients for land tenure security includes stable political environments, sound institutional arrangements, leadership, funding mechanisms, societal backing, legal frameworks, administrative and technical capacities, a supportive land information system in the form of land registries or cadastres. Is it interesting that the main point of a supportive land information system is one of the elements to support a stable land registration system. The current system in Malaysia is focused on a centralised system and only focuses on a database that has created long processes and is less transparent. Moreover, the issue of adverse possession to part parcel that could have a significant and negative effect on the operation of the land market (Williamson 2000). Therefore, there is a need to reform the land registration system to solve the glitches in the current land registration system in Malaysia.

The land registration process in Malaysia has been established since the formation of Malay States under the monarchy system, which controls several local land registration systems. In this modern day, land registration authorisation is still governed by the states. Both federal and state governments have made efforts to modernise the land registration system. As a result, the Computerised Land Registration System has been introduced in an effort to digitalise land registration in Malaysia. This system attempts to replace the previous manual system such as land registration, land administration, land searching records and other land related matters. Nevertheless, this system has merely replaced the manual system where the main characteristics are on display of the land matters information. In other words, the system is not a dynamic system which can link to different levels of management, especially for the decision-making process. Nevertheless, in 2009 the biometric system was introduced for all levels of transactions. This was another effort by both levels of government to increase the level of digitalisation in terms of land registration. As a result, a new land registration system was introduced and is known as ‘e-tanah’ (E-land). This land registration system aligns with the federal government’s initiative to implement an electronic government. As land is a state matter, this system has only therefore been implemented in several states in Malaysia. The ‘e-tanah’ system consists of several modules, namely registration, output, consent, strata, development, enforcement, auction, requisition, license and disposal.

In Malaysia, in terms of the land registration process, once the seller and owner are in an agreement and have signed the Sale and Purchase Agreement (SPA), the property is registered under two stages. The first stage is with the stamp office, the adjudication Form 14A/Deed of Assignment will be completed and submitted to the stamp office which can be done manually or online. Once this has been accepted by the stamp office

the lawyer will be provided with an adjudication number. The next stage is that the property will be valued by the Valuation and Property Services Department and a report will be prepared and sent to the stamp office for stamp duty evaluation. This process usually takes one to eight working days, depending on the complexity of the subject property. The stamp duty is between 1% and 3% of the value of the property and must be paid within 30 days from the notice of assessment date issued by the stamp office unit.

For property without an individual title, transferring of property rights from seller to buyer is considered done once the Deed of Assignment is duly executed and stamped. Deed of Assignment is a legal instrument that conveys the transferring of property rights from the seller (assignor) to the buyer (assignee). For property with an individual title, the next stage is to formally register the new ownership on the property at the state or district level land office. Documents needed at this stage include the original land title document, certified copies of the buyer's and seller's identification/passport (company Memorandum and Articles of Association for corporate buyers/sellers), stamped Form 14A and a copy of current quit rent and assessment receipt among others. The land office will endorse the name of the buyer on the land title document. This land title document will be kept in the strong room at the land office. A new land title document will be issued to the buyer. This registration process is completed within one working day from the date of complete document submission. As shown in Figure 1, there are two stages of land registration, one is the processing stage in which all the documents are processed for the validation, and after the verification, the next step is the land transfer in which the land officer transfers the land.

Blockchain is a new concept which can be classified under the impact from the Industrial Revolution 4.0 (IR 4.0). It can be classified under a public ledger where all transactions are collected in a chain of blocks. The chain will continuously grow until new blocks are attached to it. The blockchain technology has the key characteristics that are important for high quality of the storage system such decentralisation, persistency, anonymity and audibility (Zheng et al. 2018). Blockchain integrates several fundamental technologies such as cryptographic which has digital signature and distributed consensus mechanism. Most importantly blockchain eradicates fraud in payments because with blockchain technology, a transaction is able to be finished without any bank or intermediary. Blockchain can be used in various financial services such as digital assets, remittance and online payments (Peters et al. 2015). As the land registration system handles very sensitive information regarding land titles, safety and privacy issues are crucial. According to research by Forte et al. (2015), the proof of concept of Autonomous Decentralised Peer-to-Peer Telemetry (ADEPT) is a system using blockchain technologies to build a distributed network of devices. Furthermore, NRI (2015) stressed that the land information system using blockchain technology is able to improve the efficiency of public services. Other developed countries such as the US and the UK have seen blockchain of title recording system as the future of title record keeping that is able to provide a solution in terms of current recording systems (Speilman 2016).

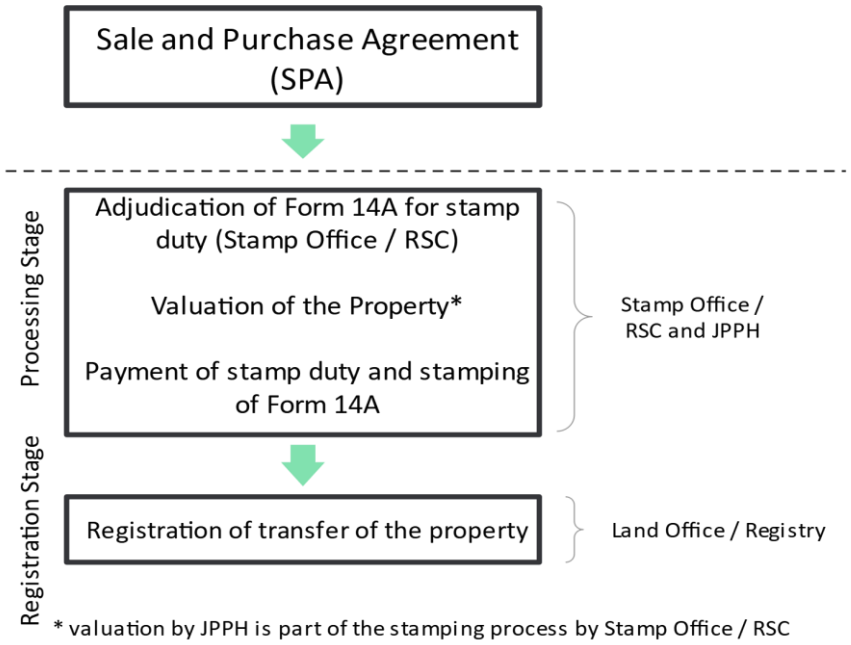


Figure 1. Land Registration Process in Malaysia

In recent decades we have seen the transition from manual to digital records and online portals. Nevertheless, the transition from manual to digital has not changed the instability in terms of system security, especially those with higher privileges that are able to access the system. In other words, a user who has high access and knows the inside security measures could change the database's state. One of the ways to avoid the misuse of this privilege is through the proper logging mechanism. Currently, the government is using traditional Relational Database Management System (RDBMS), where it manages land records. It requires the whole hierarchy of software, software engineers, and administrative staff to keep up with the data's management. The system is costly and requires a lot of technical knowledge to upgrade or to make changes. The current implementations of any financial software are built on centralised architecture. The centralised nature of the data makes it prone to issues of power. The people who have more power are able to do more damage as the data is held in a centralised place. Furthermore, even with the logging mechanisms in a centralised instrument, any person with elevated privileges can hack or attack the system and/or corrupt the logging mechanism. Consequently, it can make the person untraceable.

The data integrity means that the information which was intended in its initial state is what it remains throughout the lifecycle of the data without any changes to it. In the traditional centralised data storage, the person can change the data without any trace just by going to the backend database and changing the record with the new values. That change will break the data integrity as it will reflect two states of the same data but at different times. The land registration involves many departments such as land revenue, tax department, and many others (see Figure 1). This means that the data will be shared with the same piece of land to a different department. Each department has different angles or views to deal with the same data. The data is then added upon, and the information added needs to be updated to other departments. This leads to a duplication of data and also the data being manipulated.

Once a deed is finalised, or the land is transferred between hands, the new sale deed should reflect all the recent changes to the data. The new owner's data and the information added to the land record needs to be updated to the original piece of land. In traditional systems any missing data will make the buyer look for missing links in the documentation. For example, the revenue department does not have the correct information as the original owner is deceased and their son or daughter inherited it. This kind of incomplete information will be a hassle to solve for any buyer.

3. Methodology

The methodology of this research consists of three phases, namely land registration characteristics identification, land transfer process and performance evaluation. The first step is the initial step which initiates the process of this research. Phase 1 is the land registration in which upon client request, the land is registered. In Phase 2, the land transfer process explains how the land is securely transferred from one owner to another. In Phase 3, the proposed framework's performance is evaluated by comparing it with the existing methods.

Phase 1 of this research framework is land registration using blockchain. The primary blockchain is built. Basically, when a client wants to register a land, they have to visit the land registration office. In the land registration office, the administrator checks all the required documents of the client. After verifying these documents, the administrator contains the record in the blockchain. The land must not be already registered. If the land is not yet registered, it implies that this land is new. The administrator enters the client's public key, client id/passport, land title, and land address. If the client has no public/private keys, these keys will be generated and handed over to the client. The system will check for any previous registration with the same land title, and if none is found, then the registration is recorded in the transaction. The data is stored in two ways. First raw data as key-value pair and second as encrypted with the client's public key is also a signed copy of the record stored in the block. After the land registration, the block mining process is carried out, where the record is recorded in the blockchain.

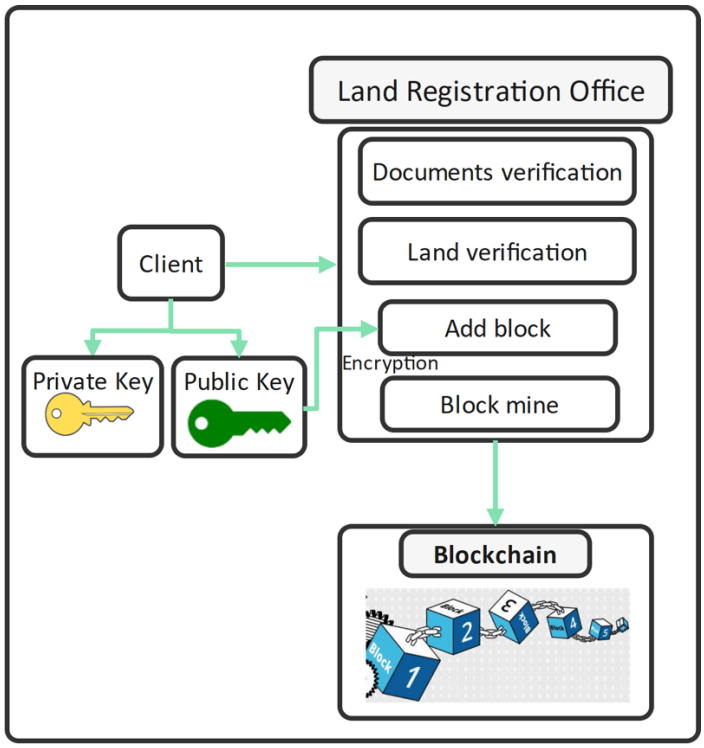
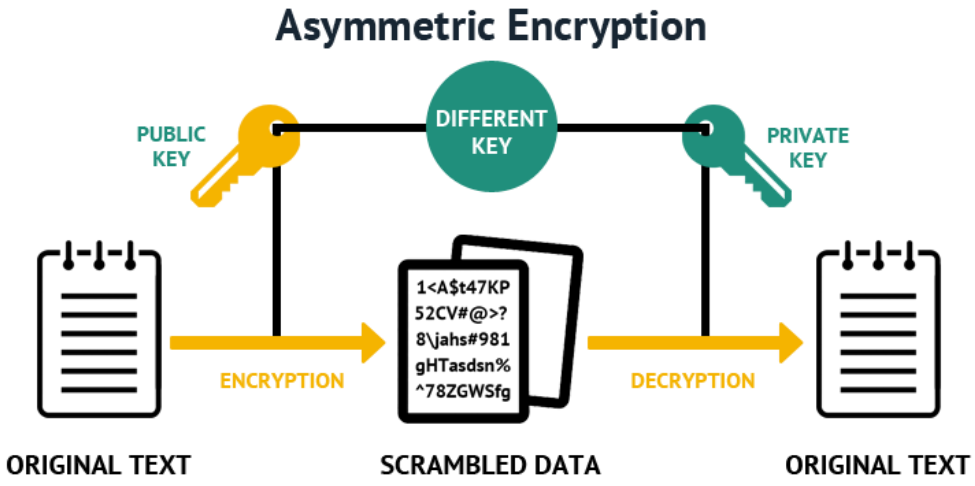


Figure 2. Secure land registration using blockchain



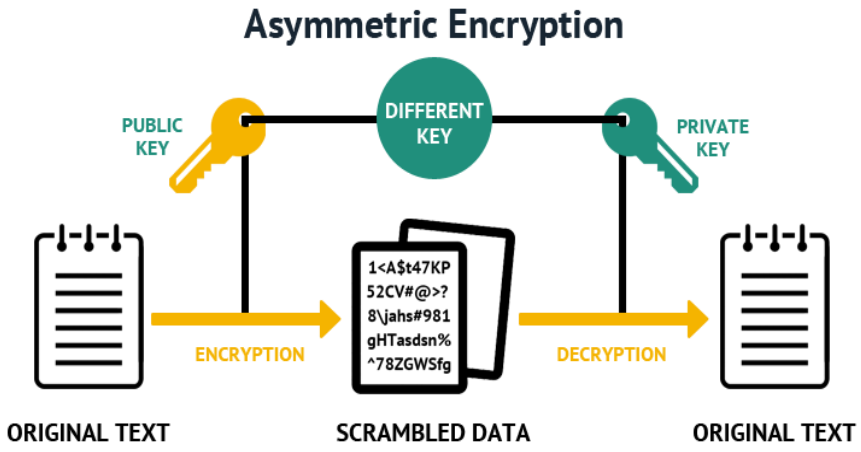


Figure 3. Asymmetric Encryption

Rivest- Shamir- Adleman (RSA) Key Generation Process

The core element in this research is to make land data secure and for that RSA public/private keys are used. The 2048 bits' length of keys is used for security. The mode for encryption used is EAX mode (encrypt-then-authenticate-then-translate). It is an Authenticated Encryption with Associated Data (AEAD) algorithm designed to simultaneously provide authentication and privacy of the message (authenticated encryption) with a two-pass scheme, one pass for achieving privacy and one for authenticity for each block.

The proposed framework is secure using the following equations 1 to 4:

Let's assume K_{PR}, K_{PB} be the private key and public key respectively,

The encryption and decryption processes are:

$$\textbf{Encrypted binary data} = \textbf{encrypt}(\mathbf{K_{PB}}, \textbf{Data}) \quad (1)$$

$$\textbf{Encrypted data} = \textbf{EncodeBase64}(\textbf{Encrypted Bianary Data}) \quad (2)$$

To reverse we have to decode and then decrypt to get our original data back.

$$\textbf{Encrypted Binary Data} = \textbf{DecodeBase 64}(\textbf{ Encrypted Data}) \quad (3)$$

$$\textbf{Plain Data} = \textbf{decrypt}(\mathbf{K_{PR}}, \textbf{Encrypted Binary Data}) \quad (4)$$

Since K_{PR} is only available with the owner and is offline, makes this more secure. The data attributed which we encrypt is based on the JSON data structure. JSON is a short form of JavaScript Object Notation. The JSON data is very flexible, and more attributes can be added as per the needs.

Block Mining

The blocks are mined after the land is registered. The mining process is distributed among peers. Whichever peer mines it announces it to other peers. Mining is used to secure and verify land transactions. Mining involves blockchain miners who add land transaction data to the global public ledger of past transactions. Mining involves doing proof of work. The evidence of work consists in finding some value on a criterion. The criteria used in this research are described as follows:

a. There is a level of difficulty involved in the mining process in this research.

b. The difficulty level to be configured by an integer value.

c. The mining process finds such hash values that begin with a zero number occurred by the difficulty.

d. There is a level of difficulty involved in the mining process in this research.

Once a difficulty level to be configured by an integer value. Once a deal is found, the proof of work is considered complete, and the block is announced and added to the list of blocks.

Blockchain

After block mining, the block is added to the blockchain. Before an announcement can be made on the network, a consensus is reached by checking the peer's current state with the stat of the connected peer. If any other peer does not do proof of work, then the following process of the announcement is initiated:

a. The announcement is made to all the peers and all other peers.

b. All peers validate the answer by computing for themselves if the hash value calculated has started with leading zeros by the difficult times.

c. Upon successful validation, the block is added in the pier blocks as well.

The next phase is the land transfer phase where the land transfer process is explained in detail. The proposed framework for land transfer is secured from the fraud of ownership because only the landowner has the right to transfer the property. Figure 4 illustrates the secure land transfer by using the blockchain concept. The framework consists of several block areas, as follows:

i. Name <= Name of the owner.

ii. Id/Passport <= national identity number or passport number.

iii. Title <= title of the land.

iv. Address <= address of the land, where the land is situated.

v. Owner public key <= RSA public key.

vi. Previous hash <= hash value of the previous block (of Secure Harsh Algorithm (SHA) 256 bits).

vii. Timestamp <= time on which the block was added.

viii. Nonce <= a bit for randomisation.

ix. Signed Data <= (This has all the above attributes encrypted using the owner public key) the purpose of this will be discussed in land transfer.

Each block owner has the right to view the block attributes and also the right to transfer the ownership to a new owner. The function to transfer the license is only given if the ownership is proven by the client by providing private keys. Even the admin cannot change the ownership once a land record is added to the blockchain.

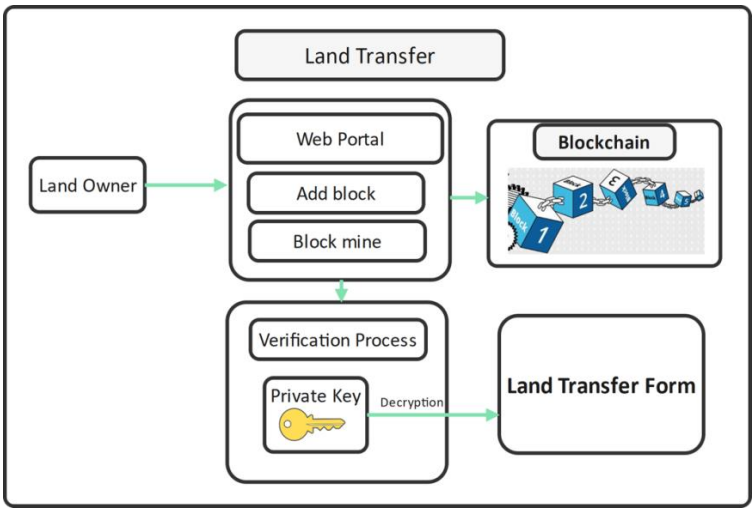


Figure 4. Secure land transfer using blockchain

Land Transfer

The second phase of the proposed framework is the land transfer. Once the administrator adds the land then that land becomes available in the blockchain. The land can then only be transferred to the new owner if the following criteria are met,as listed below:

i. The land record must be the latest one.
ii. The owner must provide their private key file.
iii. The new owner must provide their public key file.

The next phase is to validate the private keys of the old owner. This step requires the owner to input the personal key file, which will be used to decrypt the signed data. Signed data is stored in the block with all the attributes. The process is shown in Figure 5. The successful decryption of the signed data fulfils two things, and they are:

i. The owner is indeed the one who initially registered with the department (Authentication).
ii. The land and owner data are secured (Integrity).

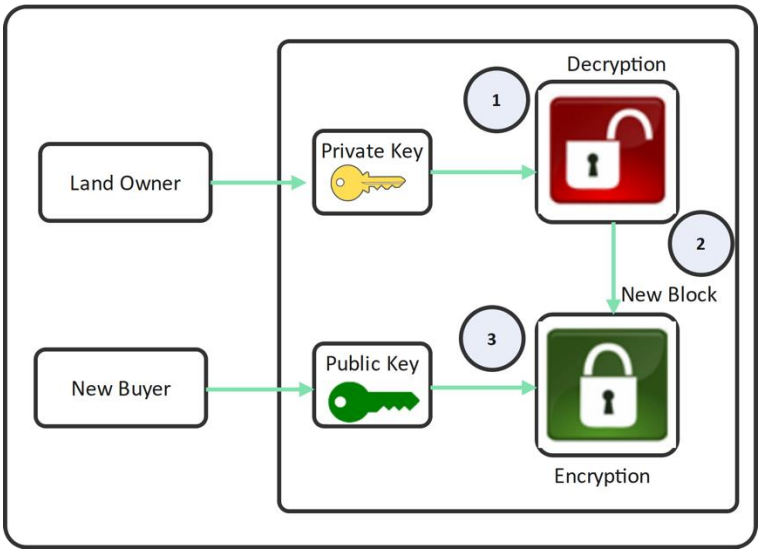


Figure 5. Secure land transfer process

Verification Process

Once the data has been decrypted, it will be verified from the original owner who has access to the system. At this stage, the land transfer process will begin here. A form will be displayed to the owner in order to give the buyer private keys, public keys, and provide name and identification information of the buyer. Nevertheless, the address and title of the land are unalterable. Land transfer begins by decrypting the signed data and getting the land title and land address from the old block using the private key of the old owner. The latest transaction will have the new owner's name and identification. This new data set is then encrypted with the new buyer's public key and the signed data will be stored in an attribute of the block. The block is then sent to the mining process to be included in the blockchain. In this process, if decryption fails, the whole verification process will also fail, which indicates that the keys are not correct and the land does not belong to the client.

Private Keys

Private keys are needed if the client wants to sell their land. The deficiency of keys indicates that the land is in a locked state and cannot be moved. This is very important to keep it back up before it could be used to encrypt. The client needs to understand the importance of keeping the keys safe. Each public key has a private counter key that needs to be protected as the loss of the private key will lead to loss of land transfer. The key generation process can be done independently from the system where generated keys are given to the admin for secure encryption of the land and owner record of the data. This process is not able to be handed to the administrator due to the administrator of the system not being able to change any ownership without private keys from the landowner. The system will not store private keys which further makes the process secure and protects against insider attacks.

Performance Evaluation

The performance evaluation will be performed using the efficiency parameter. The SHA 256 and SHA 512 will be evaluated on the 200 iterations of data. The performance evaluation of the proposed framework is performed by comparing it with the existing methods.

Design and Implementation

In this stage, the tools and technologies need to be designed. This will involve software stack in the hardware. The design of the algorithm will also need to be design based on the User Experience Design (UX) and User Interface Design (UI). The crucial steps that need to be taken to ensure the data has security are discussed in the design algorithm section. The implementations come after the design algorithm. The initial design deals with the UI/UX and the project's cases are present. Python has been selected for the implementation as it is one of the growing programming languages. Python has many libraries available for the community, which also adds a plus point in selecting this language. The web interface is also a built-in Python web framework, namely flask. The current implementation is done on Mac OS v 10.15.5 using PyCharm as IDE (Integrated Development Environment).

After the selection of language, the basics of blockchain are implemented. Two different apps are developed. One is for taking care of blockchain. The client app is written to request data from the blockchain app and provides a web interface to the blockchain server, as shown in Figure 6. The admin of the land registration would add the initial land record by adding the public key of the landowner. The landowner needs to view their land title and would also be able to transfer the land title to a new owner.

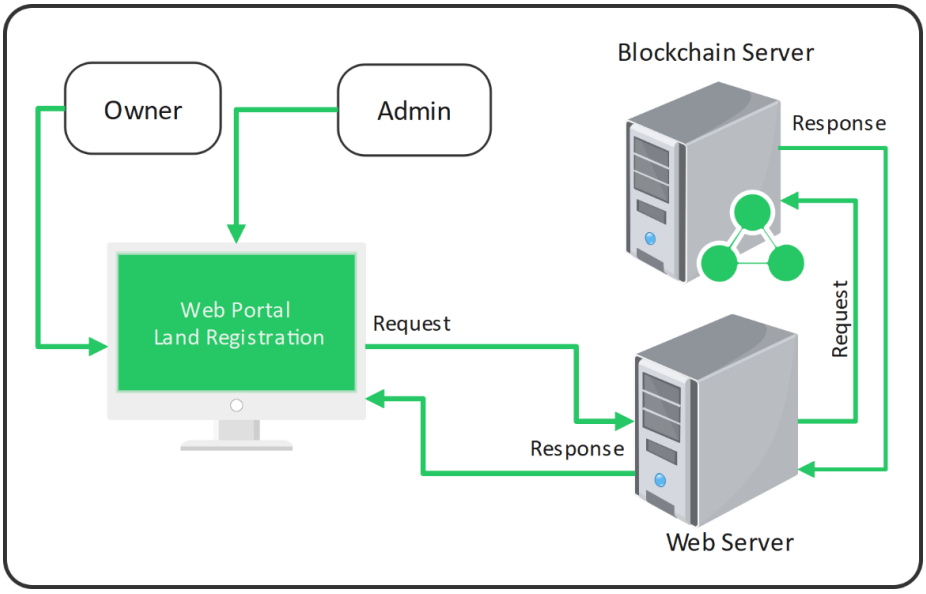


Figure 6. Overview of the proposed design

It is essential for the owner never to share their private key with anyone. The loss of the private key would mean a loss of property. If the owner wants to sell their land, the system presents the interface to give access to the owner to change the ownership. This interface assumes that the underlying country laws and regulatory rules are fulfilled, and any tax or duty is paid. After every requirement is completed, the buyer's public key should be accessible to the owner to transfer the land to the new buyer.

Class Structure and Application Hierarchy

As described, there will be two applications that run in parallel. The blockchain application runs on port 8000, and the client application runs on port 5000. These are variable ports just for running the system in the local environment. The server application has the following classes, methods, and attributes:

Class Block

This class will attribute a single block and the function to compute the hashing value of the blocks.

attribute: index

attribute: nonce

attribute: previous_hash

attribute: timestamp

attribute: transactions

function: __init__()

function: compute_hash()

Class Blockchain

This class will have the block class as a list. The unmined blocks will be added by this class. Proof of work is implemented in this class as well.

(a) attribute: chain

(b) attribute: difficulty

(c) attribute: nonce

(d) attribute: unconfirmed_transactions

(e) function: __init__()

(f) function: create_genesis_block()

(g) function: last_block()

(h) function: add_block()

(i) function: proof_of_work()

(j) function: add_new_transaction()

(k) function: is_valid_proof()

(l) function: check_chain_validity()

(m) function: mine()

The Server Flask Application

This is the server side of the application. This application interacts with the blockchain. New peers will be added by this class. Any requests from the peers will be served by this application.

(a) attribute: blockchain

(b) attribute: peers

(c) function: new_transaction()

(d) function: get_chain()

(e) function: get_chain_by_id()

(f) function: mine_unconfirmed_transactions()

(g) function: register_new_peers()

(h) function: register_with_existing_node()

(i) function: create_chain_from_dump()

(j) function: verify_and_add_block()

(k) function: get_pending_tx()

(l) function: consensus()

(m) function: announce_new_block()

The server flask application deals with all the requests made to the blockchain. Also, it takes care of the nodes connecting to the server for getting the blocks. In addition, we need an application which communicates with the client and blockchain server for that we have our **client application** with the following attributes:

(a) attribute: cached_blocks_in_the_chain

(b) function: fetch_whole_blockchain()

(c) function: fetch_block_from_blockchain()

(d) function: admin_add_land_record()

(e) function: view_block()

(f) function: decrypt_signed_data()

(g) function: index()

(h) function: submit_land_record_to_blockchain()

(i) function: transfer_owner()

(j) function: timestamp_to_string()

Although the client application can contain the RSA key generation, it is better to have separated it out to a separate **cryptography file** for ease:

(a) function: generate_keys()

(b) function: encryption()

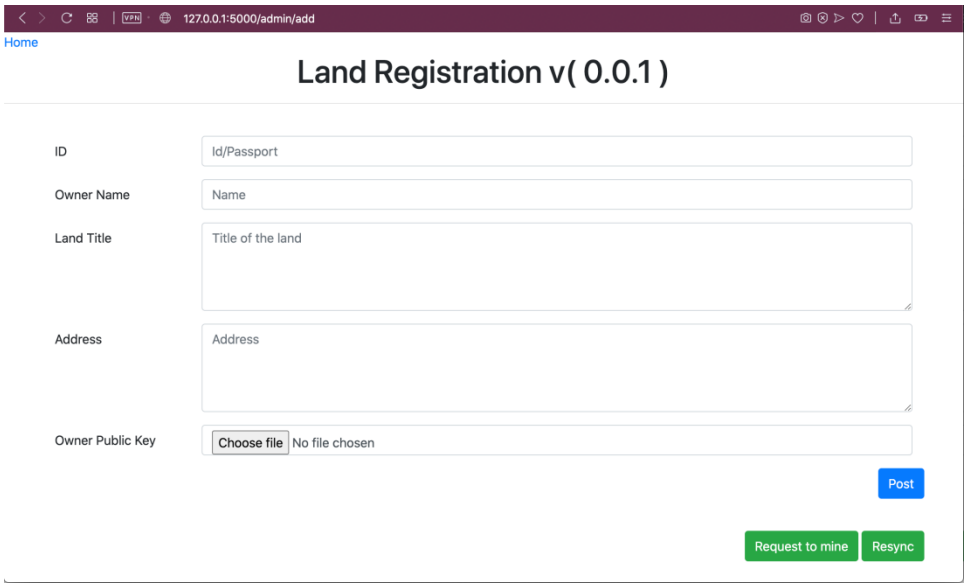
(c) function: decryption()

Admin and owner have been identified as the client. Both of the user roles have been given two different URLs to do their respective tasks. Following URL rules or URL end points are implemented in the client application:

1. 127.0.0.1:5000/index
2. 127.0.0.1:5000/admin/add <== end point for the admin to add new land record
3. 127.0.0.1:5000/view/<block_id>(integer number) <== server both methods GET and POST
4. 127.0.0.1:5000/submit <== only accept method using POST
5. 127.0.0.1:5000/transfer_owner/<block_id>(integer number) <== accept only method using POST

Admin Interface

In Figure 7, it requires the administrator to enter information such as owner id/passport, owner name, land title, land address, and the owner public key. The publickey can be generated by the owner independent



of the system or using the system. Admin can access the URL 2 mentioned above and will see the following UI:

Figure 7. Land registration/add form

Public/Owner Interface

In Figure 8, the root URL is displayed, which shows all the mined blocks. Each block index is a link; clicking on the link will open the block.

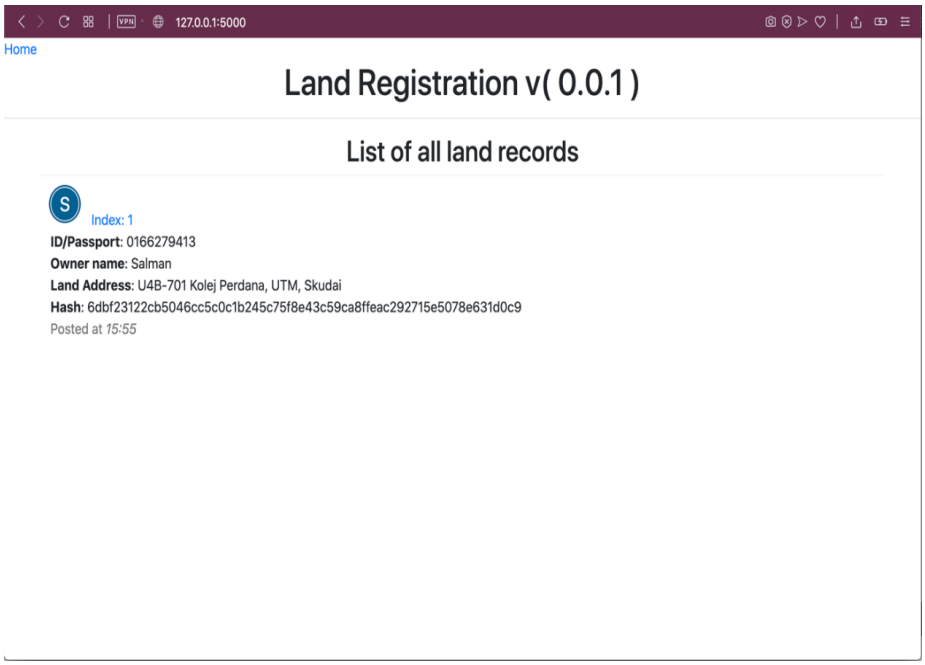


Figure 8. Index/list of all the mined/added block/land records

Figure 9 shows the detail page, this page has a link to transfer the land to the new owner, but that is blocked until the owner provides their ownership by giving the private key. Private keys are not stored in the server in any shape or form.

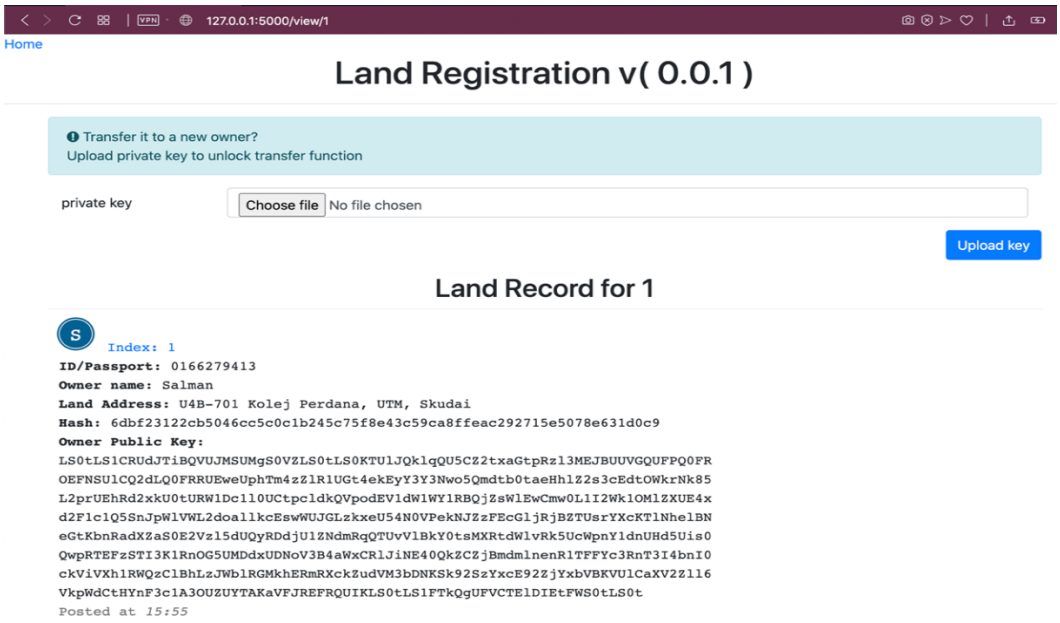


Figure 9. View a particular block by id

In Figure 10, the land transfer form asks for the new buyer's details plus the key of the old buyer and new buyer

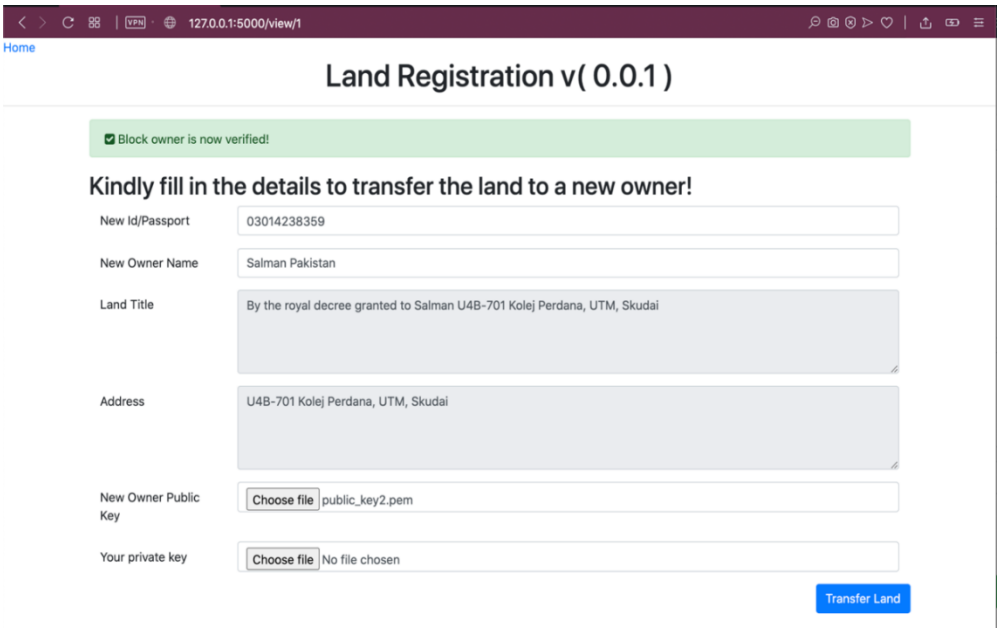


Figure 10. Land transfer form

In Figure 11, after a successful transfer, the user is able to view the new block with the new owner name and new owner id.

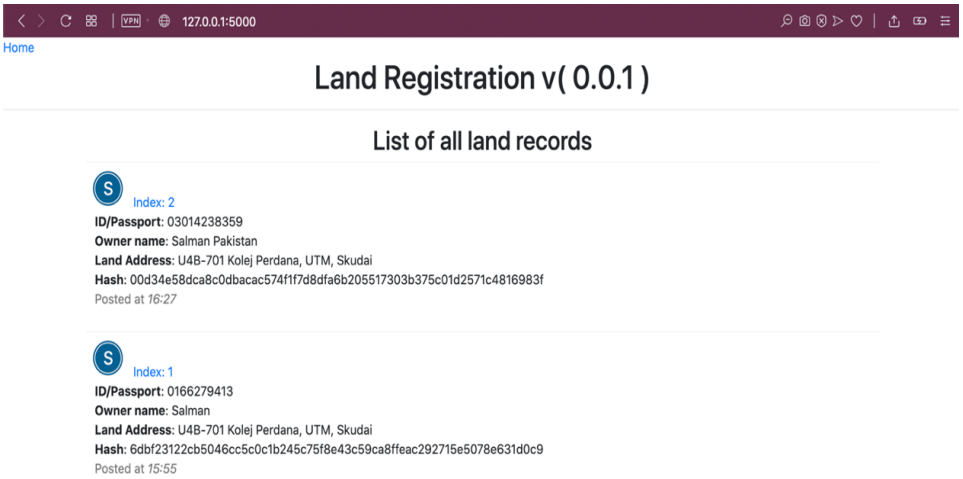


Figure 11. Land transfer success

In Figure 12, after a new owner, the old record becomes locked so any future changes cannot be performed.

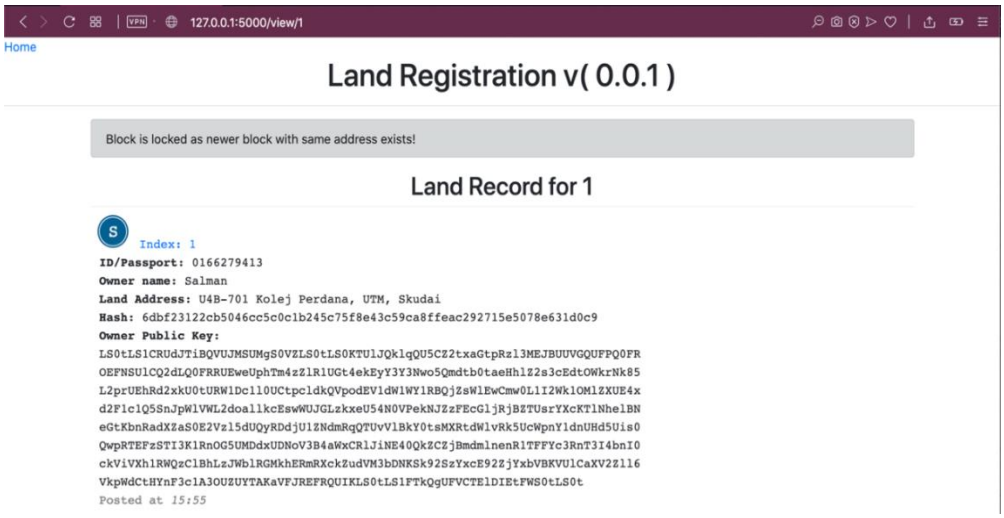


Figure 12. Locked land

Functional Algorithms

In this section, we will look into the critical elements of the code. Python community offers many libraries. This gives a remarkable ability to find applicable code and reuse it. The application is building on top of the flask web framework the version is 1.1.2. Flask gives the ability to add HTTP protocol in the implementation. Our project's important aspect relies on RSA, public-private key encryption, and decryption, and for that we have used the **pycryptodome** library.

Encryption

The following is encryption which starts by first encoding the string data into UTF-8; the public key is imported. A random session key is generated for the generation of the ciphertext. The session key will be needed for the decryption process, so we need to save the session key. That is the reason we are keeping all this information as encrypted. The flowchart of the encryption process is shown below in Figure 13.

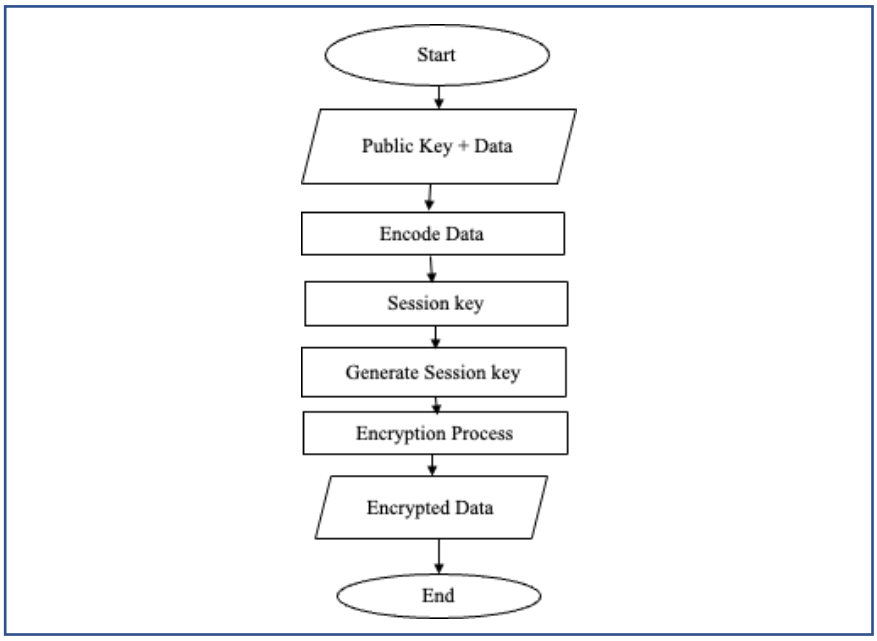


Figure 13. Flowchart of encryption process

Decryption

The decryption starts by importing the private key into the RSA library. Encrypted data is split as it was encoded with extra new lines. Then each block is identified and extracted. Once we have the session key, nonce, tag, and ciphertext from the encrypted data, that is passed to RSA decrypt to get the session key. The session key is used to get the chipper AES which is the intermediate value, and the ciphertext is decrypted to get the original data. The flowchart of the decryption process is shown below in Figure 14.

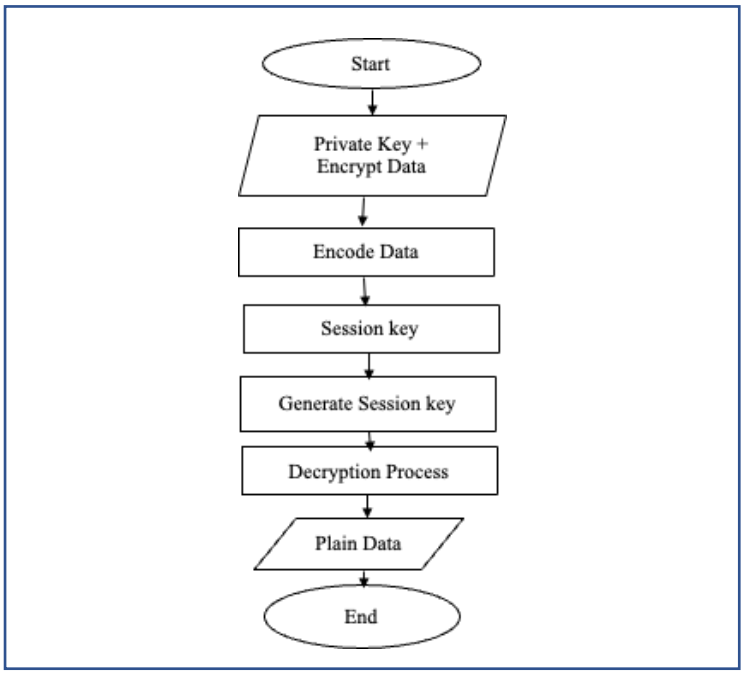


Figure 14. Flowchart of decryption process

Decryption Algorithm

The decryption works in the opposite direction of encryption in this the private key and ciphertext or encrypted data is given, and the plain text or decrypted text is returned.

Adding/Registering Land Record

Admin can submit the data of any land given where they also have the owner's public key, once the data is entered. The address is checked for uniqueness, and then the data set is encrypted using the public key and then is sent to be added to the blockchain. The flowchart of the registration process is shown below in Figure 15.

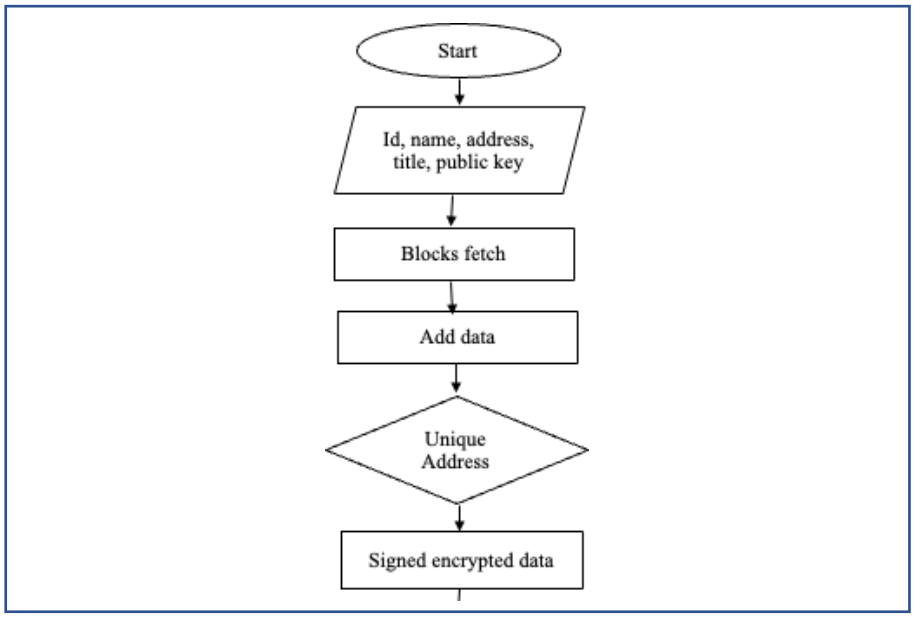


Figure 15. Flowchart of land registration process

Adding/Registering Land Record Algorithm

The land registration or additional algorithm takes the land record attributes and address and the owner's public key. The address must be unique for the land to be registered. This is to prevent any double owner problem and prevent any fraud by the insider.

Transfer Owner Land Record

The current owner’s private keys and the new owner’s public keys are required before it can be performed. Once given the data, it is then checked if the current owner is indeed the block's owner by successful decryption. After which address and title are fetched from decrypted data so that nobody can change it. New owner’s name and id are encrypted and added to a new block along with the public key. The flowchart of the land transfer process is shown below in Figure 16.

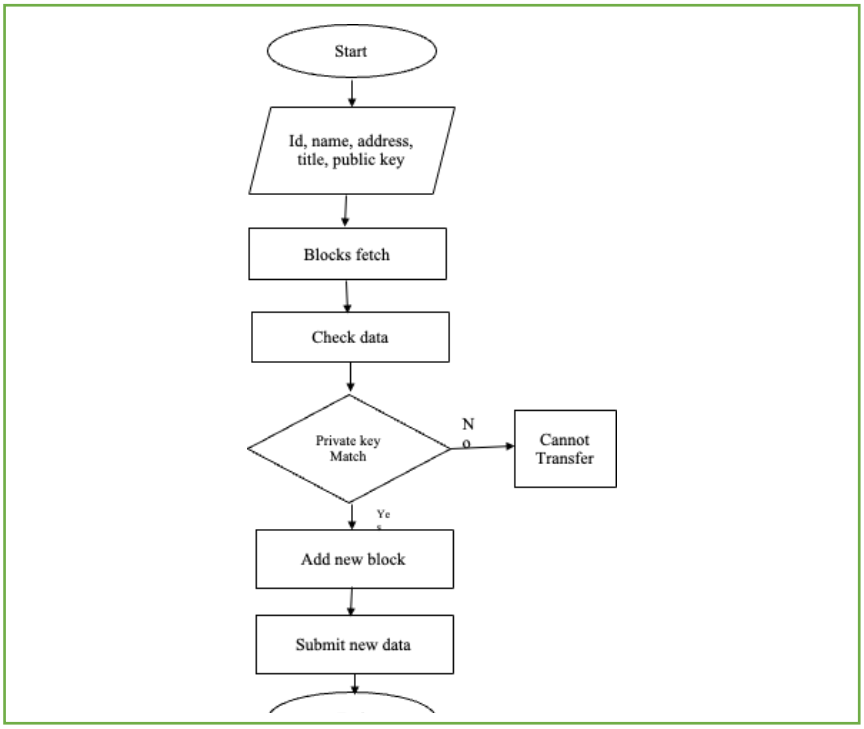


Figure 16. Flowchart of land transfer process

Transfer Owner Land Record Algorithm

The algorithm for the transfer of the land records works by taking the block id of the land record of the owner's name the old private key of the old owner and the new public key of the new owner. The block can only be decrypted by the old public key of the old owner. This is a security feature to prevent any false allotment by any third party. Only the old owner can provide the old private key.

Computing Hash Algorithm

The block is initialised with the attributes. After which the features are accessed using the internal access. Block string is computed after each feature is added in a key-value pair with JSON dump facility. Then the block string is hashed using SHA 256, and then hex digest is used. This is usually used to exchange the value safely in email or other non-binary environments. Since we are using the data in our web application over the HTTP protocol, then it is safe to use hex digest over the bits produced.

Proof of Work Before Mining Algorithm

The nonce is incremented every time our condition of hash starting with 0 is not met. This changes the hash to a new value. It acts more like a randomisation technique so that the algorithm can arrive at a satisfying condition for our proof of work and return the hash.

Is Valid Proof Algorithm

This method checks if the hash indeed starts with a 0 number that stratifies the blockchain's difficulty. Combined with the computed hash and the sent hash should be equal. These two conditions make the valid proof method.

Add block Algorithm

The block is added only if the block has a valid proof of work and the last block hash value is not equal to this hash value, which means that both blocks are different in terms of their attributes.

Mining Algorithm

The mining process is straightforward in increments indexed by one, adds all unconfirmed transactions, calculates the new hash, and is sent to the additional block. All the unconfirmed transactions are then cleared to avoid the duplication of the duplicate transactions added twice.

Check Chain Validity Algorithm

The chain is only considered valid as long as the block and its hash are correct, and also the previous hash is not equal to the new hash.

Consensus Algorithm

In the consensus method, we are using a simple approach if any other peer has the longest chain, others will accept it. This is the bare bone minimum for our project and needs to be updated for any production environment.

Validation

The proposed framework of land registration system by using blockchain has been validated by using 200 blocks of data. Each data block consists of 3008 bytes or 24,064 bits of data. The total size of blockchain becomes 200 x 3008 bytes is 587.5 Kilobytes of data. The data attribute we stored in the block is id, name, title, address, owner public key. This research has used SHA 512 due to performance and security improvement compared to SHA 256. Figure 17 tabulates the comparison of the performance between SHA 256 and SHA 512. The graph below contains 200 iterations of hashing of data; the orange line depicts SHA 256 processing time, and the blue line represents SHA 512. The high orange line shows more processing time while the subtle blue line represents quick hashing done by the SHA 512. The vertical axis represents the time in seconds it took to complete the hashing by both SHA functions on the blockchain’s identical data blocks. The graph also shows that the SHA 512 is more efficient in hashing than the SHA 256.

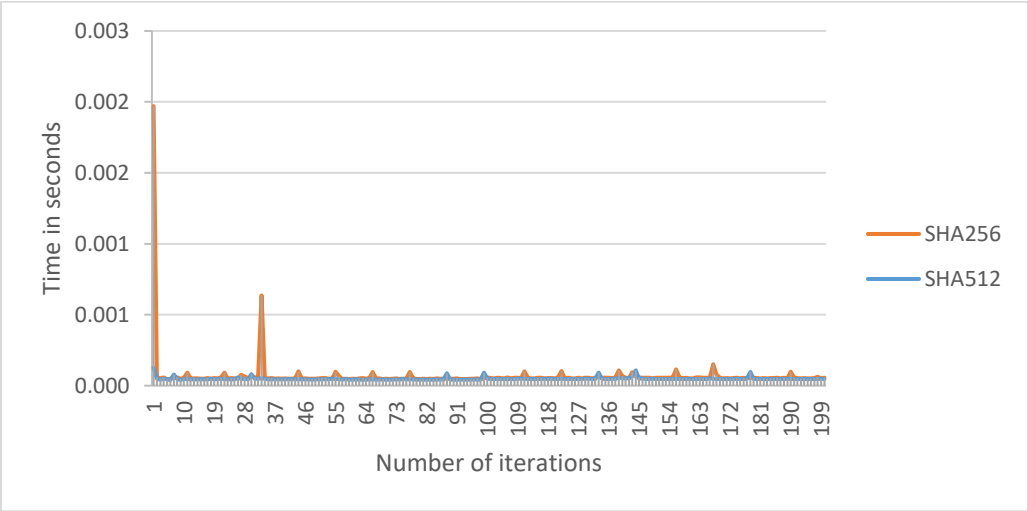


Figure 17. Performance graph between SHA256 vs SHA512

The improvement achieved by using SHA 512 is calculated by taking the average time of both hashing functions. The average time of SHA 256 is observed to be 0.0000689232349395752 seconds, while the average time of SHA 512 is followed to 0.0000483262538909912 seconds. The difference between the two is calculated by subtracting SHA 256 – SHA 512. The percentage change was calculated using the equation as follows:

$$\%\ \mathbf{Change} = \mathbf{100}\ \times \frac{(\mathbf{Hash\ Time_{512}} - \mathbf{Hash\ Time_{256}})}{|\mathbf{Hash\ Time_{256}}|}$$

$$= \mathbf{100} \times \frac{(\mathbf{0.0000483262538909912} - \mathbf{0.0000689232349395752})}{\mathbf{0.0000689232349395752}}$$

$$\%\ \mathbf{Change} = \mathbf{-29.883944170}\ \%$$

The calculated percentage of change is -29.8%. The negative sign indicates a decrease in time for SHA 512 when compared with SHA 256. This means that the SHA 512 is more efficient compared to SHA 256. The real improvement gained from using SHA 512 is 29.8%, which is better than SHA 256.

Comparison with Existing Methods

The proposed framework is also compared with state-of-the-art methods. Table 1 represents the difference between the enhancement suggested in this work with the previous ones. This proposed framework shows a better enhancement in performance and cryptographic security improvement compared to the previous work. The existing works in Table 1 are using the SHA 256. The reason for using SHA 256 is due to the legacy

system and hardware. The legacy systems are 32-bit architecture, and SHA 256 performs better over it. It is costly to upgrade all the legacy software and hardware to the relatively unknown 64-bit architecture. The SHA 512 is more cost effective than SHA 256 when used on the 64-bit computing devices (Gueron 2012). The industry uses SHA 256 due to its backward compatibility on the 32-bit computing devices. These 32-bit devices are used in servers and legacy systems, which will take some time to be replaced with new 64-bit computing devices. Our results in Table 1 also indicate that the SHA 512 over the 64-bit architecture performed far better than 32-bit architecture.

Table 1. Difference between the proposed frameworks

Works Compared	**Proof of Work**	**SHA 256**	**SHA 512**
Sankar et al. 2017	YES	YES	NO
Turkanović et al. 2018	YES	YES	NO
Sajana, M.; Sethumadhavan, M. 2018	YES	NO	NO
Krishnapriya & Sarath 2020	YES	YES	NO
Proposed Framework	YES	YES	YES

The hashing technique in the proposed framework gave better results. The SHA 512 internally uses 64 bits which for its initial hash values and round constants and the modern CPU architecture is 64 bits. The same bits give SHA 512 advantage when used over 64-bit architecture. That is one of the key reasons for the performance gain we were able to achieve. The industry standard for hashing used in state of the art is SHA 256 (Krishnapriya & Sarath 2020; Turkanović et al. 2018). Due to the performance gained from the SHA 512 will be beneficial to the overall time saving of each transaction.The proposed framework secures the data with the asymmetric keys, and fraud is prevented due to the hashing and encryption of the data. This, combined with the improved performance of SHA 512, gives it an extra edge.

1.0 Conclusion

This research attempts to provide solutions in land registration in Malaysia by using blockchain technology. There are various previous works done for secure land registration. Most of the researchers used databases such as SQL for data storage. In using these databases, secure storage cannot be maintained due to insider attacks. The proposed framework is able to prevent insider attacks and frauds. The transparency and decentralisation nature of blockchain has helped us to secure data. In terms of secure data, storage is achieved by the asymmetric cryptography of public and private keys. These keys make sure that only the original owner

can transfer ownership securely and effectively. Furthermore, this study also compares the existing frameworks which aim to improve the current practice in terms of land registration. The efficiency parameter is used by validating the performance of the proposed framework. The use of SHA 512 instead of SHA 256 has performance gains of ~30%. This will benefit the government by reducing paper and carbon emissions as well as the carbon footprint. The proposed framework is also improved by adding the Merkel tree, which will benefit the integrity and validity of data, reduce the disk space, and information needed to be transmitted over the network. The other aspects of the project that could improve are the reporting tools for all the land records which are being recorded. The secured data in our proposed blockchain can be further optimised using various compression techniques. This will allow the blockchain size to be reduced. This reduction in data will help reduce network traffic. Also, this will help the load on nodes. Furthermore, different encryption methods can be explored for asymmetric keys such as elliptical curve cryptographic algorithms.

Author Contributions: all authors contributed equally to the present work

Funding: This research received no external funding

Acknowledgments: Not applicable

Conflicts of Interest: The authors declare no conflict of interest

References

1. Vos, J. (2016). Fraud in The Netherlands, despite a transparent land registry system. Possible preventative measures and advices taken and given by the Dutch Registrar. In XIX Congreso Mundial de Derecho Registral=: 19th World Land Registration Congress: Chile, 2014 (pp. 872-930). Tirant lo Blanch.
2. Hoxha, V., & Sadiku, S. (2019). Study of factors influencing the decision to adopt the blockchain technology in real estate transactions in Kosovo. Property Management.
3. Shiller, R.J. (2005), Irrational Exuberance, Princeton University Press, Princeton, NJ.
4. Simbizi, M. C. D., Bennett, R. M., & Zevenbergen, J. (2014). Land tenure security: Revisiting and refining the concept for Sub-Saharan Africa's rural poor. Land use policy, 36, 231-238.
5. Williamson, I., Enemark, S., Wallace, J., & Rajabifard, A. (2010). Land administration for sustainable development (p. 487). Redlands, CA: ESRI Press Academic.
6. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.
7. Peters, G., Panayi, E., & Chapelle, A. (2015). Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective. Journal of Financial Perspectives, 3(3).

8. Forte, P., Romano, D., & Schmid, G. (2015). Beyond Bitcoin-Part I: A critical look at blockchain-based systems. IACR Cryptol. E Print Arch., 2015, 1164.
9. Spielman, A. (2016). Blockchain: digitally rebuilding the real estate industry (Doctoral dissertation, Massachusetts Institute of Technology).