Journal of Education for Pure Science
Vol.15, No.2 (2025)
DOI: https://doi.org/10.32792/jeps.v15i2.425
Website: jceps.utq.edu.iq Email: jceps@eps.utq.edu.iq

Enhancing Security of Real Estate Registration Through Block chain Technology

Najlaa Mohammed Karem *[1], Kadhim Hasen Alibraheem[*2],

College of Education for pure science / University of Thiqar ,Thi-qar, Iraq
[2] College of Education for pure science / University of Thiqar ,Thi-qar, Iraq

*Corresponding email: najlaamohammed.23co3@utq.edu.iq

Received 25/ 6 /2024, Accepted 8 / 8 /2024, Published 1 / 6 /2025

Abstract

Decentralized environments are necessary for the complex and sensitive data required for land registration. The main focus of present technology is database storage, which is less secure and prone to fraud. This is because unstructured data and non relational databases present challenges due to the characteristics of the database. Fraud is one of the main problems and a persistent issue with the Malaysian land registration system public ledgers are created by block chain technology from all complex transactions, which hold great promise for replacing intricate systems with a single, straightforward database. As a result of current land office procedures, the land registration process is highly centralized, requiring multiple people to evaluate and authorize the data. Consequently, it is necessary to determine the block chain technology model.

Keywords: Block chain, Encryption , Real statement, PoW

1- Introduction

Real estate transactions have undergone a significant transformation in the digital age, ushering in a period of never-before-seen complexity and ramifications. This change has caused a significant movement towards online platforms, and as a result, the real estate sector is adopting more and more different types of electronic commerce, or "e-busine[**Abualhamayl et al.2023]** These technologically **adva**nced digital platforms are crucial for increasing the precision and effectiveness of monitoring and documenting real estate activity. The recorded history of these operations is captured by real estate provenance, which includes information about prior owners, transaction histories, and any other historical context pertaining

to the real estate's origin**. [Saull et al., 2020]** Precise provenance monitoring guarantees openness and fosters confidence but also provides a host of advantages like risk reduction, fraud avoidance, and assistance with making well-informed decisions availability of precise Having comprehensive historical data makes it possible to analyze the market and find investment opportunities. Notwithstanding these benefits, there are a number of obstacles to overcome when attempting to preserve transactional integrity and validate historical data in real estate transactions.[**Zhang et al., 2023]** Finally the aim of work is to improve real estate e-business reliability by employing block chain technology to accurately and transparently record property provenance. Furthermore, GREP improves security by shielding transactional data from tampering and unwanted access by leveraging block chain's built-in characteristics. Moreover, the essential component of GREP's architecture is the full engagement of governmental organizations. This involvement extends beyond only adhering to regulations. As we'll talk about later, it also guarantees greater standards of responsibility in real estate transactions. In the end, GREP creates the groundwork for reliable and safe real estate e-business transactions.

A COMPARISON OF BLOCKCHAIN AND CONVENTIONAL DISTRIBUTED DATABASE STORAGE.

Comparison factor	Traditional distributed database	Blockchain
System management	Multiple copies of the database are kept in separate locations, but it is overseen by a single server.	Every participant stores complete copies of the blockchain and maintains it.
Data accessibility	The entire database is inaccessible to common participants.	Blockchain is open source and available to all users.
Function execution	Data computation and collecting are handled by a central server.	After a smart contract, each participant can create and record new data.
Cost	All processing and storage are done on a single server.	Each participant bears the expense of computation and storage.
Communication	Mostly, participants communicate the central server alone.	Every participant disseminated updates to all other participants.
Participants privacy	Information must be sent to the central server to foster confidence.	Completely operational in an anonymous environment without any established trust

Data security	single-point failure on the central server; if the central server is compromised, data may be altered or erased.	No single point of failure and immutability of data once saved on blockchain

Thanks to these benefits blockchain has proven remarkably successful in cryptocurrency applications like PeerCoin [7] Ethereum [6] and Bitcoin [5]. The present blockchain ecosystem is growing as blockchain technology is embraced by an increasing number of industries. Financial ledger systems [8] the Internet of Things (IoT) [9–10] edge and cloud computing [11–13] public administration [12–13] healthcare [14–15] and supply chain [16–18] are a few industries that have developed block chain enabled solutions. This paper is structured as follows: Section II presents a summary of previous published research on securing real estate registration. In contrast section III provides an explanation of the recommended system approach. The experiment results and the recommended systems effectiveness in securing real estate registration were discussed in Section IV. The papers inclusion section will serve as a conclusion to all of this.

This paper comes with some important contributions illustrated as follows:

1) Make real estate registration more secure.

2) Used AES to encrypt the real estate information including the buyer seller and document information.

3) Storing real estate information using Poof of work block chain technology.

4) Using the Minutiae algorithm and the fingerprint feature to gain access to the authentication system.

5) Software interaction is made easier by Graphical User Interfaces (GUIs) which arrange features visually. They provide accessible customizable and simple navigation which boosts user happiness and productivity.

2- RELATED WORK

Among the difficulties Shinde et al. face are land conflict issues that put owners entire rights in jeopardy. In Indias centralized land registry system 2019 [16] is mentioned. The potential for double spending and fraud forgeries were among the problems with the current system. By utilizing block chain technology the proposed framework addresses these issues. This innovative platform aims to solve the shortcomings of the current system by providing a secure and efficient means of storing and retrieving property documents. The system also contains features that notify the document owner in case of unauthorized access ensuring a permanent

and secure record. 2021 will see Yadav and co. described a method for utilizing blockchain technology to build a safe transparent fast and space-efficient framework for property registration. This improved framework presents an algorithm with an impressive 96 that complies with MRRCM. a 48 percent gain over the PoW strategy and a block generation rate of three times faster. 6% in contrast to the round-robin approach. The land registrys query process is now more efficient thanks to a modified hashtag table search algorithm that makes use of blockchain technology. A significant improvement of 59 is seen in the average search times. Comparing the broad line search method with the actual results the percentage dropped by 18. 68 percent when using this hash search technique in comparison to the hash table approach. Shashikant et al. presented a novel real estate transaction procedure that makes use of blockchain technology to improve efficiency and transparency. in 2022 [18]. The landowner initiates the transaction by verifying their identity through a blockchain-enabled web portal. After communicating with a real estate agent online the seller signs a secure contract. Consumers expedite and save time by independently verifying who owns the property via a web or app. Following an in-person examination of the property an appraisal of the asset is added to the blockchain for bank approval. The agent and bank have direct access to data including inspection reports thanks to the blockchain.

For parties with permission blockchain-based smart contracts execute the sale and produce a permanent digital contract. Verifying and issuing the Certificate of Ownership request is made easier for the government by using the web/app. The blockchain-based Certificate of Ownership creation and registration combined with automated stamp duty and charge calculations produce a digitalized decentralized process that significantly enhances the real estate transaction process overall. Blockchains inherent security and transparency features as described by Shrivastava et al. 2023 [19] proposed developing a land registration system with the help of technology. The three main features of blockchain technology—permanence decentralization and immutability—offer chances for cost savings and improved efficiency. The suggested approach comprises building a d

ecentralized application with a focus on developing and executing smart contracts using the Ethereum network. Part of the implementation involves creating frontend web pages using Next and React. For server features and routing use js. Drawing from the analysis and conclusions presented in the paper this proposed methodology for developing a secure and efficient land register system is considered feasible and effective.

THE PROPOSED SYSTEM

The process starts with a login page for user authentication. To comply with standard security protocols users must input their username and password. Biometric authentication through fingerprint recognition is also used to strengthen access control. The minutiae algorithm is used to process this biometric data guaranteeing a safe and dependable means of identity verification. After completing the authentication process successfully users can enter estate information such as buyer and seller details estate numbers and pertinent dates. Data encryption is essential to protecting sensitive information. The entered data is hashed using the SHA-256 algorithm to make it unintelligible to unauthorized parties. To further strengthen the secrecy of documents pertaining to estates the AES algorithm is used to encrypt uploaded documents and real estate information during this process. . . To guarantee that the data entered is accurate and true authorized staff members are responsible for cross-checking the details. By entering the system with their given login credentials employees can review and validate the encrypted estate information. This ensures that only authenticated and verified data is processed further and uploaded to the blockchain. A transparent and uncrackable bookkeeping system is

created by adding the validated estate facts to a blockchain network. The proof of work consensus method is used to validate each block before it is added to the blockchain creating an immutable record of real estate transactions. Through this connection the likelihood of fraud or manipulation is diminished by guaranteeing the traceability and integrity of data related to estates. as depicted in Figure 1. For example each color in this figure illustrates the proposed system structure and the operation of a block chain. Blue illustrates how to finish the process if the fingerprints match in the process Red indicates that the process is not successful and Green indicates that the process is successful.

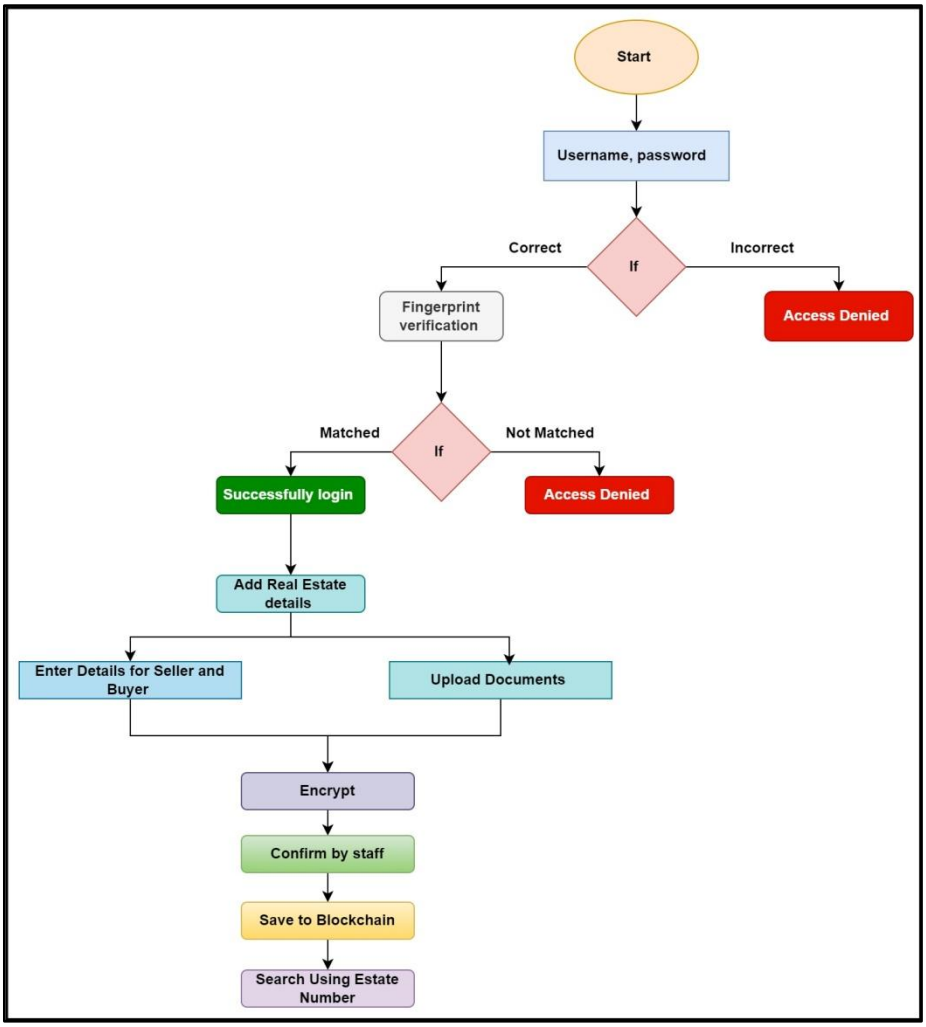


Fig. 1. Overview of the proposed system structure.

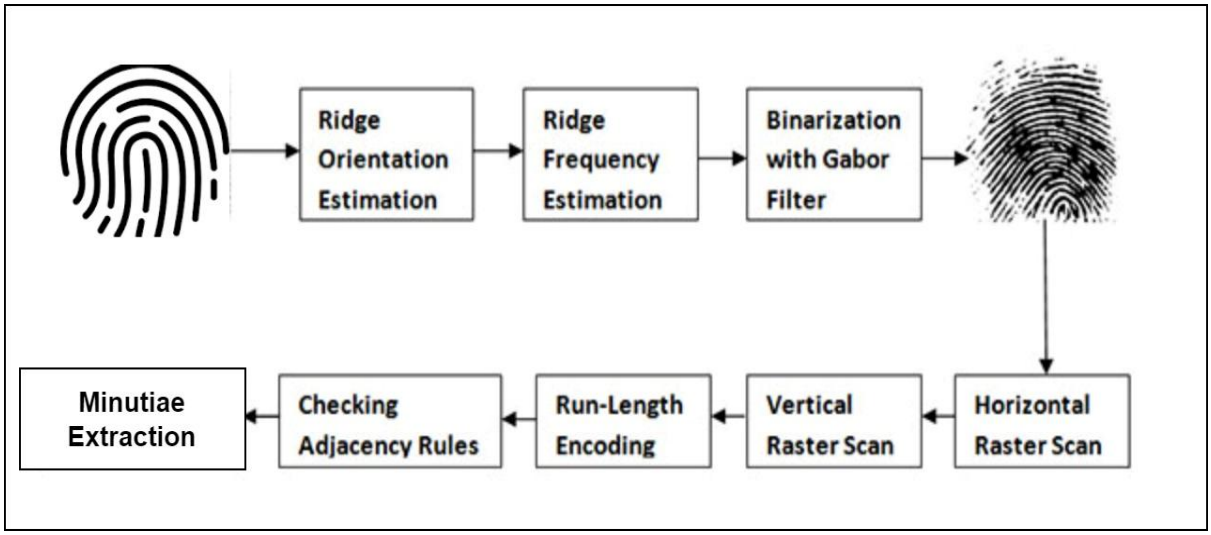
A. Fingerprint process.

This methodology makes use of both vertical and horizontal run-length encoding techniques as well as binary fingerprint images. Without requiring computationally intensive thinning procedures this method accelerates the extraction of minutiae. Typical fingerprint images are identified by examining the proximity of these runs which are represented as a sequence of runs following run length encoding. However not all identified characteristic runs match real minutiae so geometric limitations are needed for verification. A. Figure 2 displays the finer points of this minutiae extraction technique. To make the image better it is first pre-processed. Segmenting the image to isolate it from its background and then normalizing it to produce a preset mean and variance are the steps involved in this process. Using Gabor filtering ridges aligned with the local orientation are enhanced after the local orientation and ridge frequency surrounding each pixel are determined. As a result the contrast between the foreground and background ridges increases and noise levels decrease. After that the image is binarized which entails selecting a threshold value to classify pixels

as either white or black. Adaptive image binarization is utilized to determine the optimal threshold for each segment of the image in order to attain precise classification. When it comes to binary or labelled images run-length encoding works wonders because it maximizes processing speed while utilizing less memory. Minute-by-minute fingerprint verification offers a number of benefits over alternative methods. First of all it provides robust authentication since the unique minute point patterns remain constant across impressions made of the same finger ensuring reliable verification even in the event of variations caused by factors such as pressure or minor injuries. This resilience contributes to the increased security and accuracy of biometric authentication systems. Minuties-based techniques are further characterized by their small template size making them suitable for efficient transmission and storage in large-scale applications such as law enforcement and border control.
[20].

Fig. 2. Minutiae algorithm process for fingerprint identification.

A. Encryption and Hashing



The Advanced Encryption Standard algorithm and hashing algorithm used in the proposed system are SHA-256. SHA-256 is a system that strengthens trust security and transparency in real estate systems by hashing passwords to improve user account security [21 22]. A unique 256-bit hash code or signature can be obtained for any given text or data using this hashing technique. To verify the datas integrity the generated hash value must be compared to a predefined reference value [23]. SHA-256 is a member of the Secure Hash Algorithm 2 (SHA-2) hashing algorithm family. A private cryptographic hashing process is used by the Secure Hash Algorithm 256 (SHA-256) to generate a 256-bit output [24]. The AES algorithm is used to encrypt and decrypt the data. By using encryption data is converted into cypher text an understandable format. Conversely decryption transforms the data back into its original form which is called plain text. [26].

B. Poof of work

Proof-of-work (PoW) is a crucial technique in block chain networks especially when adding new data to the blockchain. Every time a network member wants to add a new batch of transactions to the blockchain the transactions are compiled into what is called a block. Around this block the PoW procedure revolves. Proof-of-work (PoW) systems operate on the fundamental concept of a nonce which is a unique value that is used only once and is typically a 32-bit arbitrary number. Until a hash from the combined data (transactions and nonce) meets predefined criteria miners iteratively adjust the nonce in the block. A fixed-length string of characters is created as this hash. . The hash that is generated must above all satisfy a set of specifications called the target value. The threshold that a legitimate hash must fall below is set by this target number. It is an indicator of how challenging the network is. To maintain a constant block generation rate while taking into account the networks total processing power the difficulty level is regularly adjusted. . . Mining is the process of locating a valid hash and it requires a lot of processing power. Miners continuously compute hashes using their computing power alternating between various nonce values until one is found that meets the requirements of the target value. The PoW algorithm is based on this process of looking for a valid hash which is a representation of the labor that miners perform. Once the hash satisfies the target value requirements the miner broadcasts the new block to the network. Nodes within the network autonomously verify the authenticity of the PoW by hashing the contents of the block with the provided nonce and ensuring that the resulting hash matches the intended value. Through this decentralized validation mechanism the PoWs legitimacy is verified. as many nodes in the network concur.

C. Add New block.

Proof of Work is a protocol that enables the addition of a block to an existing block chain by selecting transactions using nonce manipulation to compute a valid hash independent network node verification consensus formation and rewarding miners. As seen in Fig. 3 this complex process ensures that consensus is reached and the proof of workability of block chain networks. The new block is appended to the chain of blocks and upon verification the associated transactions are deemed verified as well. The miner that successfully completes the block receives a block reward which is typically cryptocurrency in addition to any transaction costs included in the block. As algorithm 1 has demonstrated.

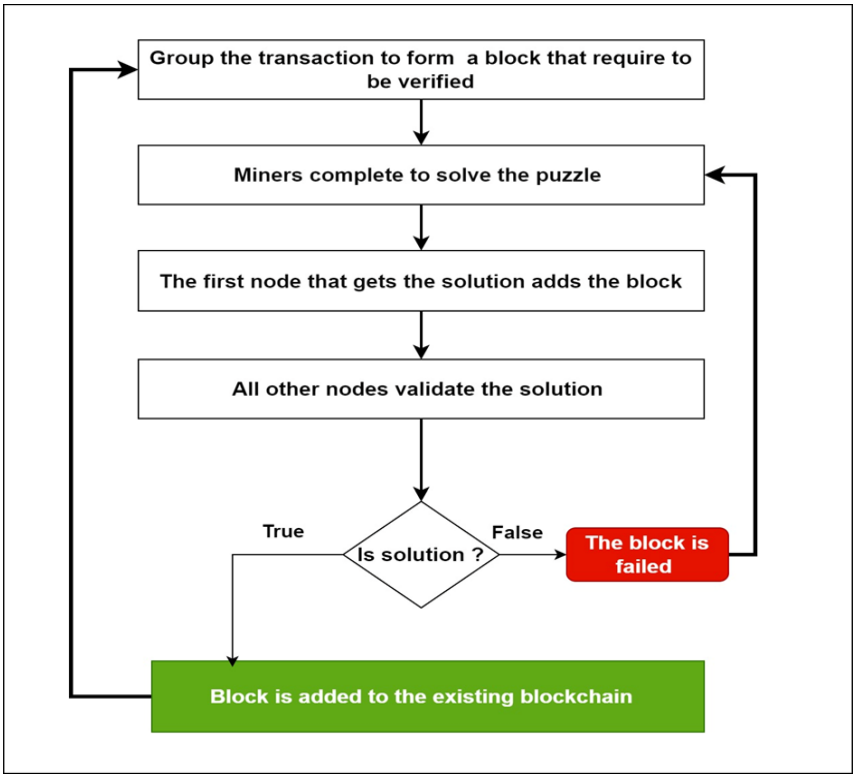


Fig. 3. Proof of work diagram.

Algorithm 1: Implementing a Basic Blockchain

Input : Add transaction for real estate
Output: Add these real estate details to blockchain

Begin

Step 1: define Block structure:

Initialization: index, timestamp, data, previous hash, nonce.
Calculate hash of the block.

Step 2: Implement method to mine the block.
Define Blockchain class with attribute: chain.
Initialize chain with a genesis block.
Implement method to add a new block to the chain.
Implement method to validate the integrity of the blockchain.
Step 3: Mining new blocks:
Initialize a new block with index, timestamp, data, and previous hash.
Mine the new block by finding a nonce that produces a hash meets the difficulty criteria.
Add the mined block to the blockchain.
Step 4: Validating the blockchain:
Iterate through each block in the chain starting from the second block.
Verify that the hash of each block matches the hash of the previous block.
Verify that the nonce of each block produces a hash meeting the difficulty criteria.
If any block fails validation

The blockchain is considered invalid.
Else
Data add to the blockchain.
End If
End

imentation set up.

1) **Application.**
2) To implement this system the Python programming language was used. Since Anaconda Navigator was installed the Python programming language could be accessed using a Jupyter notebook.
3) **2) Hardware.**
An Intel Core i7-8565U processor and 16 GB of RAM are part of the setu

3- Methodology

The land transfer process feature identification for land registration and performance evaluation are the three phases of the Block Chain technique. The first step is the action that initiates this research procedure.[Alsamhi and others. 2019].

The land transfer procedure explains the first phase which is land registration in which the land is registered at the clients request. Phase 2 describes the safe transfer of land between owners. Phase 3: A comparison of the proposed framework with the current approaches is used to assess its efficacy. The initial stage of this research framework involves land registration through blockchain technology.

Constructing the primary blockchain?To register a piece of land a client essentially needs to visit the land registration office. The administrator at the office of land registration confirms that the client has sent in the required paperwork. [Andersson along with others. 2020]. The administrator is in possession of the record on the blockchain once it has been verified. It isnt currently listed as land. If the land is not yet registered it is assumed that it is newly acquired. The land address land title client ID or passport and public key of the client are entered by the administrator. [The Reurink et al. in 2018]. If the client does not already own the public and private keys they will be generated and given to them. If the system does not find any previous registrations with the same land title the registration is recorded in the transaction. In Koven et al. [2019]. The data can be stored in two different methods. Included is a signed copy of the data that has been encrypted using the clients public key after being initially stored in raw key-value pair format. document stored in the block. Once the land has been registered the record is mined for blocks on the blockchain. [Shepherd et al. in 2020]

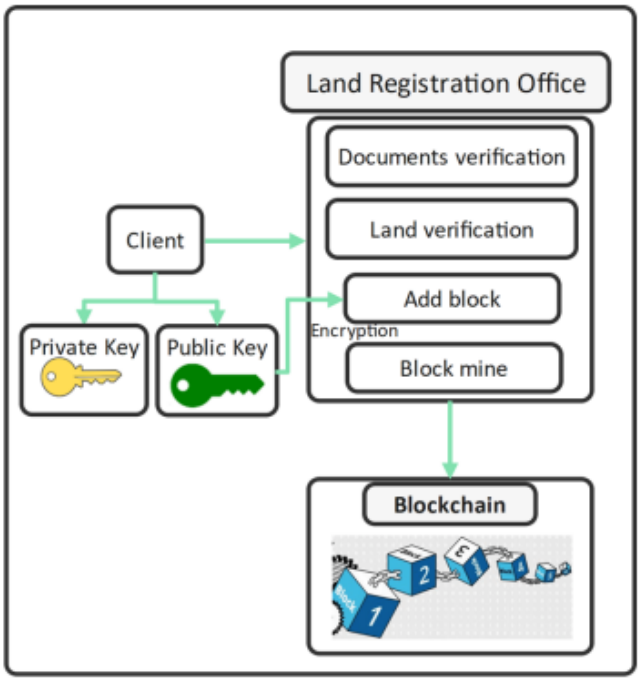


Figure 4.Secure land registration using blockchain. [Nadel et al., 2020].

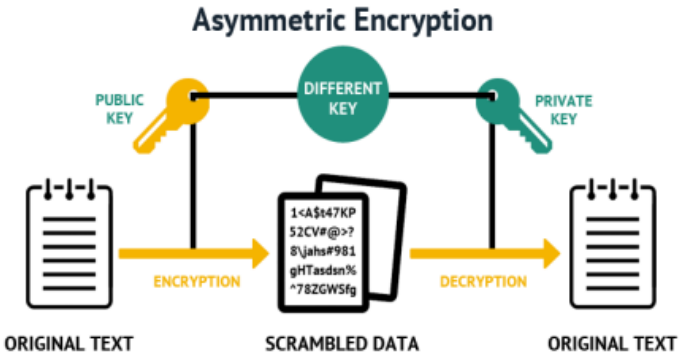


Figure 3. Asymmetric Encryption.

The [RSRivest Shamir and Adleman] Key Generation Technique. The primary objective of this research is to secure land data and RSA public/private keys are used to accomplish this. Keys that are 2048 bits long are used for security. The encryption method used is called EAX mode (encryptthen-authenticate-then-translate). The technique is known as Authenticated Encryption with Associated Data (AEAD) algorithm. designed with a two-pass scheme—one for achieving privacy and another for confirming the authenticity of each block—to provide message privacy and authentication (authenticated encryption) at the same time. According to [Kumar et al. 2021] The suggested frameworks security is demonstrated by equations 1 through 4 below. Assume KPB is the public key and KPR is the private key.

The encryption and decryption processes are:

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

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

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

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

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

This is more secure because KPR is only accessible with the owner and is offline. The JSON data structure serves as the foundation for the attributed data that we encrypt. The abbreviation for JavaScript Object Notation is JSON. Because of the JSON data's great flexibility, extra properties can be added as needed**. [Rana et al., 2022].**

3.1. Block Mining

After the land is registered, the blocks are mined. The procedure of mining is divided among colleagues. Any peer that mines it notifies the other peers about it. Land transactions are secured and verified by mining. Block chain miners use their mining to contribute land transaction data to the worldwide public ledger of past transactions. [**Ramasamy et al., 2021].**

Mining requires proving one's labor. Determining a value on a criterion is the proof of work.

The following describes the criteria that were applied in this study:[Rehman et al., 2022].

a. certain amount of difficulty is associated with the mining process in this study.
b. An integer value that will be used to configure the degree of difficulty.
c. These hash values, which are the result of difficulty and begin with an integer zero, are found via the mining process.
d. There is some complexity involved in the mining process used in this study.
after the assignment of an integer number to a difficulty level. Once an agreement is reached, the proof of work is considered completed and the block is declared and added to the list of blocks..
The block is appended to the blockchain following block mining. By comparing the present condition of the peer with the linked peer's stat, a consensus is formed prior to making an announcement on the network. In the event that another peer fails to provide evidence of work.[**Ramasamy et al., 2021].**
the announcement procedure starts as follows: (Jeong et al., 2021).
a. All peers and other peers are informed of the announcement.
b. Each peer verifies the response by calculating if the estimated hash value began with leading zeros during the challenging periods.
c. Once the validation process is successful, the block is also added to the pier blocks.
The next step, the land transfer phase, offers a thorough breakdown of the land transfer process.
The suggested structure for land transfer is protected against ownership fraud by the fact that only the landowner has the ability to transfer property. The secure land transfer using the blockchain concept is shown in Figure 4.
The framework is divided into the following block areas: [Auqibet al., 2021]
i. Name = The owner's name.
ii. ii. Passport/ID \= Passport or national identity number.
iii. iii. Title = land's title
iv. Address \= the land's address, which is its location.
Owner public key <= RSA public key, section IV.
vi. prior hash <= prior block's hash value (using the 256-bit Secure Hash Algorithm (SHA)).
Time stamp <= the moment the block was added in section vi.
vii. Nonce \= a little bit for randomization (viii).
ix. Signed Data <= (This is encrypted using the owner's public key to preserve all the aforementioned qualities; the reason for this will be covered in the land transfer).

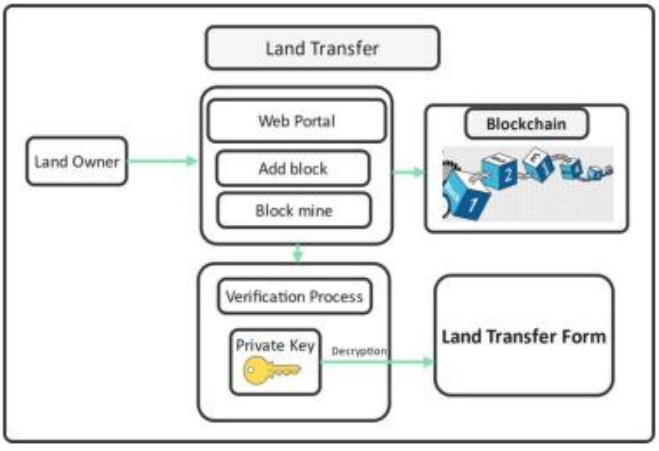


Figure 5. Secure land transfer using blockchain.(Garcia et al., 2020).
Every block owner has the ability to assign ownership to a new owner and to see the block attributes. The ability to transfer a license is contingent upon the customer proving ownership through the provision of private keys. Once a

land record is added to the blockchain, ownership cannot be changed, not even by the admin**. [Karamitsos et al., 2018].**

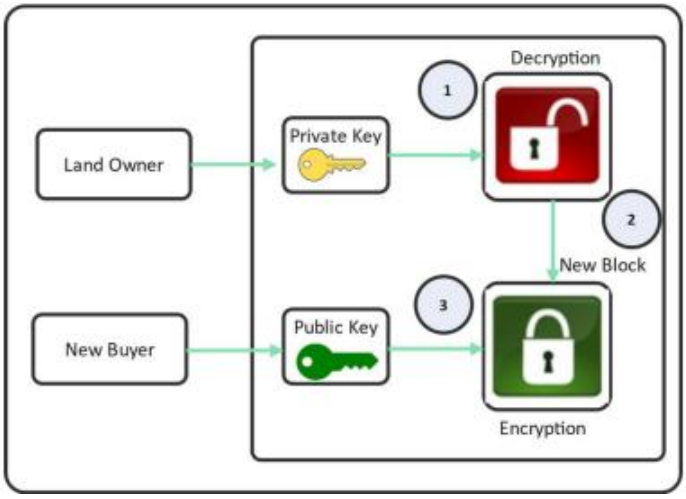


Figure 5. Secure land transfer process.(Huh et al., 2020).

Verifying the previous owner's private keys is the next step. The owner must enter the personal key file in this phase in order to decrypt the signed data. All of the properties are stored in the block containing signed data. The steps are displayed in Figure 5. Two goals are achieved by successfully decrypting the signed data:

and these are: [Tapas et al., 2020].

i. It is true that the owner registered with the department in the first place (authentication).
ii. Owner data and the land are protected (Integrity).

3.2. Design and Implementation

The technologies and tools must be designed at this point. Hardware and software stack will be involved in this. Additionally, the User Interface Design (UI) and User Experience Design (UX) must be taken into consideration when designing the algorithm**. [Woudaet al., 2019]**

The essential actions that must be performed to guarantee the security of the data are covered in the section on design algorithms. The design algorithm is followed by the implementations. The project's scenarios are included, and the UI/UX is the focus of the first design. Python is one of the growing programming languages, hence it was chosen for the implementation. **[Hoxha et al., 2019]**

Python's abundance of community-available libraries is another benefit of using this language. Additionally, the web interface has a built-in Pythonweb framework—specifically, flask. The present implementation is carried out with PyCharm, an IDE (Integrated Development Environment), on Mac OS v10.15.5. **[Zheng et al., 2018].**

4-RESUITS

Table. 4.1: Results of the proposed model cryptography

ID	Users	Users' fingerprints	Results	
1.1	A		Index	1
			Data	E4276DA40EBE7D2BD057A3E5F562B65BE6C89B8AD95A733DACBAD4B986025070
			Previous hash	075c27741a3506846368fa6e5b3477f85b31ceee71a5716e2f12b40fa21d23aa
			Self-hash	002baa43ef3c188490594b0e30f1adcb
			Nonce	645
2.1	B		Index	2
			Data	C8895DE22357F4E65186E431DEED5F41E078EDCA5CF7331FEF2E926E001E9744
			Previous hash	002baa43ef3c188490594b0e30f1adcb
			Self-hash	007d0bc057bc5524ff8aade14ccc7da1
			Nonce	476
3.1	C		Index	3
			Data	C143BD57A8EE37D8D631738E9B56EB0B87044E2D433E78B0CB2F7ED1B2A980AD
			Previous hash	007d0bc057bc5524ff8aade14ccc7da1
			Self-hash	007a5a17466ac6e97a4543f2e00dd540
			Nonce	455
4.1	D		Index	4
			Data	07CA9BEB6616924240AEF08F5021987658FA98219A74A479A942E0E20663B969
			Previous hash	007a5a17466ac6e97a4543f2e00dd540
			Self-hash	005ebda340d42868942245418699cec2
			Nonce	16
5.1	E		Index	5
			Data	5228299BC0809E7D9B1B01CD521836D1B60FFFBA32DF2B0500F050978ECEA97D
			Previous hash	005ebda340d42868942245418699cec2
			Self-hash	005c9212e41ea715b1bec6dece8680f7
			Nonce	108
6.1	F		Index	6
			Data	50BBF4C4F3593FA6A575BC6B02B66E8060D49AE37E9A978C7C2D66CF8A8BA766

			Previous hash	**00c7b013fe24705d46dbf55b8ad3c776**
			Self-hash	**00f6a5eca4c187aa465841e3d4a45cd5**
			Nonce	**382**
7.1	**G**		**Index**	**7**
			Data	**60421B8897D321BD795BC5A0E84C8A42C898FED38406DDD6D545CB1EF971CBCB**
			Previous hash	**00f6a5eca4c187aa465841e3d4a45cd5**
			Self-hash	**002f940f075ccce15935a6dc99ae2968**
			Nonce	**1234**
8.1	**H**		**Index**	**8**
			Data	**DEBF6BFBFF646211D23AF0A2E09E76CD774CC38FACB472010D6D7AEE0E7710AE**
			Previous hash	**002f940f075ccce15935a6dc99ae2968**
			Self-hash	**001b6f05523702558781a1fb1978ca77**
			Nonce	**639**
9.1	**I**		**Index**	**9**
			Data	**9908BBFD4C60C0CF3F3EE0D266C4B4D7C44DE3373791C9BEEFC076F1D0A7350E**
			Previous hash	**001b6f05523702558781a1fb1978ca77**
			Self-hash	**0021b045d8fe3c873738173a56e3ab47**
			Nonce	**155**
10.1	**J**		**Index**	**10**
			Data	**9CBFFCA22EADEDD54920C1F7B987509294B3C7C336530D19C3381795286FB426**
			Previous hash	**0093f1c6cd92ab263e5b4fa6b7fc24b8**
			Self-hash	**004f247e4f2a181d2356fed590c94ae0**
			Nonce	**67**

In table (*4.1*) one fingerprint per individual is used, but when the model is running, the encryption procedures are repeated with unique results for each fingerprint.

4.1. The Experimental Results with POW

This section presents the results obtained from applying the POW algorithm that was used in the block mining process. Different results were obtained in (Nonce), which represents the number of attempts to obtain the required hash in addition to the time taken to add each block and the total execution time. The results can be summarized in the table (4.*2*).

Table 4.2: POW's time results

Block. No	Nonce	Time to add one block/s
1	**645**	**0.1488**
2	**476**	**0.2612**
3	**455**	**0.4147**
4	**16**	**0.3997**
5	**108**	**0.4234**
6	**382**	**0.1852**
7	**1234**	**0.1982**
8	**639**	**0.2902**
9	**155**	**0.1995**
10	**67**	**0.1770**

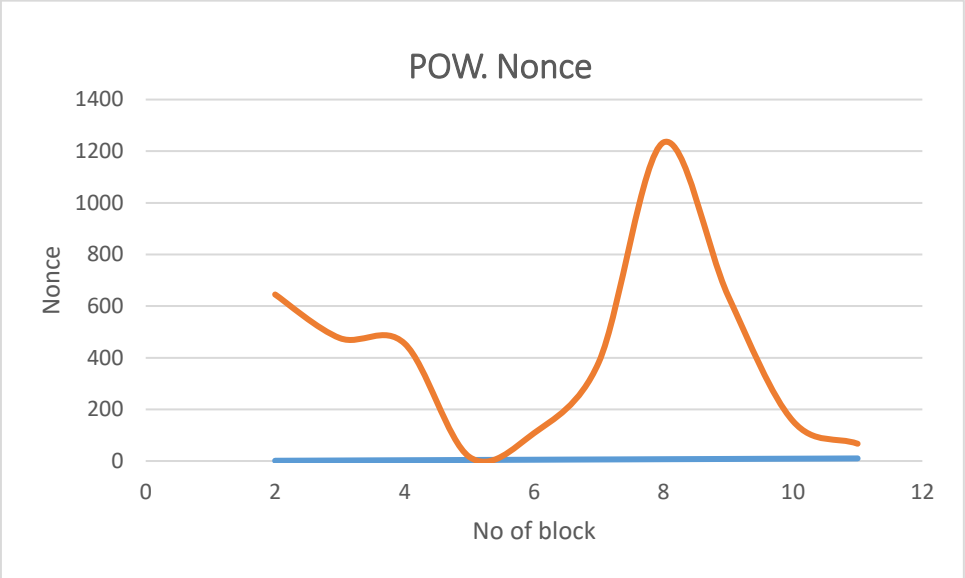


Figure 4.2: POW's nonce

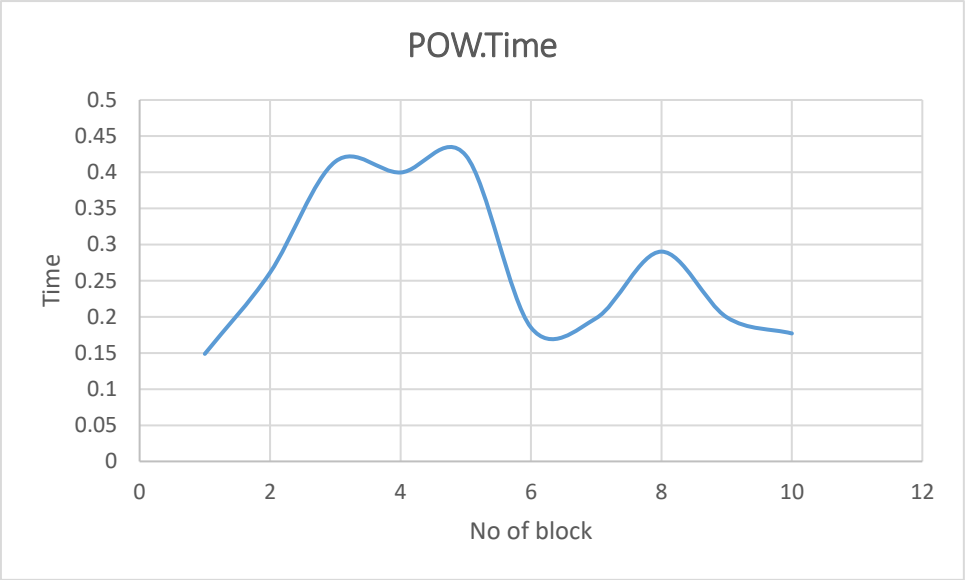


Figure 4.3: POW's time

Table (4.2) shows that the time and (Nonce) vary from one block to the next since the time is unaffected by the quantity of miner tries or efforts required to acquire a valid block.

4.2. Comparing the Proposed Model with other Studies

In this section, the proposed thesis is compared to other studies concerning the security requirements offered by BC technology, When comparing a proposed model for securing real estate registration using blockchain technology with other studies, Analyze the technologies employed in other research, noting any variations in blockchain platforms or deployment methods, Compare security measures and vulnerabilities identified in other systems, highlighting strengths and weaknesses, Evaluate how other systems facilitate user engagement and ease of access, Compare compliance strategies and challenges faced by other blockchain applications in real estate, Look at cost studies from other research to gauge economic viability.

In reference [*77*], The article proposes a set of measures, the implementation of which would improve the implementation of the Blockchain technology to modernize the registration of rights to real estate and real estate turnover. The main hypothesis of the study is the assumption that the wider use of the Blockchain will increase the reliability of the register of real estate rights and make the circulation of real estate more secure. The article identified and characterized the vectors of modernization of real estate registration using the Blockchain have been identified and characterized. The regional aspect of introducing Blockchain technology for registering rights to real estate and improving legal regulation has been considered. The use of virtual reality and augmented reality technology for real estate accounting has been proposed, through the creation of a virtual real estate registry.

Reference [*78*], The general hypothesis is that, in theory, blockchain could solve some significant challenges the real estate sector is facing, such as nontransparency, inefficiencies, fraud and corruption, high costs, and trust issues. However, the literature focuses on blockchain's theoretical benefits, challenges, or concepts. This research aims to understand the recent developments in the blockchain literature, specifically in the real estate sector, and to understand the current real-world applications by collecting empirical evidence from blockchain studies.

In reference[*79*], This paper proposes a blockchain-based real estate investment model and presents a detailed description of the real estate register authentication aspect of the model. The model uses blockchain technology to create tamper-evident records of real estate transactions and provide secure authentication and verification for

informal real estate transactions. Meanwhile, each real estate transaction is recorded in a block, and all transaction records are kept on the blockchain. This means that inventors can access these transaction records and verify their authenticity and validity. The system can also use smart contracts to automate the process of real estate transactions, which further improves transaction efficiency and reduces costs.

Reference [80], In this research, a system based on blockchain technology is proposed to create and implement a smart contract to facilitate the work of the system. It is implemented on the Binance Smart Chain platform to keep estate property records and to prevent manipulation and fraud. The system uses the keccak256 algorithm to create a unique hash for each bond based on its information. This hash helps to verify the validity and integrity of the transaction and to ensure that there are no two identical bonds. The proposed system is designed for Baghdad estate registration as a case study that uses formal information as practical implementation and as the initial stage for developing the whole system. The system increases reliability and makes the circulation of real estate transactions transparent, efficient, and secure. Table (4.3) shows the comparison of the proposed system with previous studies in terms of security requirements.

Table. 4.3: Comparison of our system with other studies

Security requirements	**References**				
	[77]	[78]	[79]	[80]	Our system
Integrity	✓	✓	✓	X	✓
scalability	✓	X	✓	✓	X
Confidentiality	✓	✓	✓	✓	✓
Availability	x	✓	X	X	x
Verification	✓	✓	✓	✓	✓
Authentication	✓	✓	✓	✓	✓
Authorized	✓	✓	X	X	✓
User control	✓	✓	X	✓	✓
Non-repudiation	✓	✓	✓	✓	✓
Decentralized	✓	✓	✓	X	✓
Privacy	x	✓	✓	✓	✓
Reduce storage	x	X	x	X	✓

5- Evaluations and Discussion

To verify the security and scalability of the blockchain-based real estate management architecture, three types of attack simulations were introduced. We carried out this first attack by modifying the block data, thus deliberately altering the state inside a block. For example, we revised either their name or the details of it to put fake news about it on the blockchain. This kind of attack aims to harm and lower the quality level of data stored in the model that will lead to disputes or scam transactions.

The second targeted block hashes, which are cryptographic fingerprints ensure immutability and the integrity of the blockchain.

Since blocks are linked using their preceding block's hash, when we changed the value of a given block's hash to alter its nature, it became impossible for this chain link in the chain as a whole. Is to compromise the entirety of the blockchain and therefore make it possible to be altered or manipulated without consent.

To recreate a Denial of Service (DoS) attack, we sent the model an unrealistic number of requests or data inputs to overwhelm it. An example would be submitting lots of malformed data to exceed the limits set on a model or attempting numerous invalid logins. If a DoS attack is victorious, the model would be out of service or block it is access to authorized users leaving users able not use it and causing troubles in one`s work which could cause monetary losses or damage reputation. As shown in Figure 5.12.

We timed different actions, primarily the blockchain's block creation process, to evaluate the overall performance of the model. We learned more about the effectiveness and scalability of the model by keeping track of the amount of time needed to mine each block. We also compared how long it took to perform various attack types, including as denial-of-service assaults, block hash modifications, and block data manipulation. By comparing the two, we were able to assess how each assault affected the resilience and functionality of the model, pointing out weaknesses and potential areas for development. The model taken a faster time to add blocks where it takes 1 second as shown in Figure 5.13.

6- Conclusion

The suggested framework's performance is validated using the efficiency parameter. There is a performance boost of about 30% when using SHA 512 instead of SHA 256, By lowering paper use, carbon emissions, and the carbon foot print, this will help the government. The Merkel tree, which will enhance data validity and integrity and lower disk space requirements and information needed to be sent over the network, is another addition that improves the suggested framework. Various compression strategies might be employed to further improve the secured data in our proposed block chain. This will enable a reduction in the size of the block chain. Network traffic will be reduced as a result of this data reduction. This will also lessen the strain on the nodes. Additionally, many encryption techniques, including elliptical curve cryptography, can be investigated for asymmetric keys.