Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Check for updates

Secure Framework for Land Record Management using Blockchain Technology

Sarah Alyounis[1], Muhammad Mehboob Yasin[1]

[1] *Department of Computer Networks, College of Computer Sciences and Information Technology, King Faisal University, Hofuf, Saudi Arabia.*

ARTICLE INFO

Article History

Received: 10-04-2023
Revised: 30-05-2023
Accepted: 12-06-2023
Published: 13-06-2023

Vol.2023, No.1

DOI:
https://doi.org/10.63180/jcsra.thestap.2023.1.3

Corresponding author.
Email:
mmyasin@kfu.edu.sa

Orcid:
https://orcid.org/0000-0003-0013-743X

ABSTRACT

Blockchain technology has become wide usage technology that can be integrated to variety of applications in different sectors to enhance the performance, security or to add a layer of implementation with specific features. In some cases it replaces the traditional type of existed systems to provide a solution to specific concerns such as the case with land record system. In this research, we provide a brief introduction of the blockchain technology in land administration, analyzing some of existed and proposed frameworks for land administration systems through a systematic review and summarize the results. Also, we highlighted the main benefits of the blockchain technology and the most important vulnerabilities in blockchain platforms. Also, we proposed a private blockchain framework using Hyper- ledger Fabric and highlighted the main reasons to choose such a platform for our system and how it can solve the double spending and tampering issues. Finally, the objective of this research is to provide mechanisms that solve the security issues to answer the research questions and develop and verify the effectiveness of our proposed framework.

Keywords: Blockchain, Secure Framework, Hyper-ledger Fabric, Threats, Cybersecurity.

How to cite the article
Alyounis, S., & Yasin, M. M. (2023). Secure Framework for Land Record Management using Blockchain Technology. Journal of Cyber Security and Risk Auditing, 2023(1), 19–48. https://doi.org/10.63180/jcsra.thestap.2023.1.3

1. Introduction

The revolution of information technology and development of applications that enhance and facilitate processes of variety sectors and systems. Most of departments and information systems transform from traditional systems to digital systems utilizing new technology. Blockchain is not a new technology, but it has new applications different sectors such as Internet of Things (IoT), healthcare, governmental systems, and land record system. Some of the existed systems required potential work with specific technical requirements to be either transformed from traditional to digital systems or to be integrated with new technologies, systems that are used to record, maintain, process, and store data. Land record systems need a transformation for the data systems to keep data updated, and protect data from manipulations, modifications, and preserve data confidentiality, integrity, and availability. Database systems need a technology that is specifically enhances the process and computational complexity, maintain records and process data to prevent any data tampering or fraudulent. Blockchain is one of the technologies that is solved the problem of traditional record systems, where it is used in land record systems as digital ledger for recorded information to enable involved parties to share, verify, validate, secure, and make transactions through secure framework. Blockchain has fundamental properties that are required to overcome the concerns of traditional system, such as immutability. Immutability is one of the main advantages of blockchain, means data cannot be deleted or changed after being stored in the blockchain which is required for data records to preserve data integrity [1]. In our research, we will design framework to represent land records as non-fungible tokens (NFT). We will build prototype of the proposed framework on Hyperledger Fabric. Building use cases to validate the framework at the end on the implementation.

This research provides a complete blockchain-based framework for a land record system that is mainly concerned to solve the highlighted issues in the existed system which are double spending, and tampering. The implementation of this research will only concern with implementation of the framework layer of the system and include manual transaction to test the system at the last stage. The remaining part of this research is organized as follows. In section 2, we provide a theoretical background of the blockchain technology and its integration to the existed systems and highlight the most important vulnerabilities in the blockchain platforms. In section 3, we described the research methodology that is used in this research and the databases included in the research process. Also, we provide our research questions that are the base of the research. In section 4, we provide a systematic review of the related work. Following with section 5, we clarified the selected blockchain structure and platform that will be used in the proposed framework, following with the main tasks of the framework implementation. Finally, in section 6 we provide work plan of the research implementation, followed by the conclusion.

2. Theoretical Background

Blockchain technology as defined by National Institute of Standards and Technology (NIST): “Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company or government)” (NISTIR 8202) [2]. Blockchain technology is not a new invitation, with security concerns and technology development blockchain technology has new applications to different domains such as land administration systems. Due to the blockchain characteristics which will be discussed in section 2.1, blockchain-based land administration frameworks are proposed to solve the current security vulnerabilities of existing land administration system which are double- spending and mutability [3][4]. The usage of blockchain technology improve the security and trust of transactions by using decentralized database where only verified transactions are stored in the blockchain, improve, and maintain data integrity by providing immutability using cryptographic hash function. Also, it will reduce the fraudulent by prevent unauthorized access using peer-to-peer networks. Along with the important benefits that are provided by blockchain, it has different structures based on the type of the framework and access: public blockchain, private blockchain, and hybrid blockchain, as shown in Table 1 [5]. Some researchers highlighted that hybrid blockchain would be more beneficial for land administration systems, where the system can have the security features of private structure and type of access of the public blockchain [6].

2.1 Blockchain Characteristics

Blockchain technology provides important features that that enhance and affect, and improve the development and security when it is adopted by land administration systems [4][7][8]: - Decentralization*:* Decentralized blockchain means that the blockchain architecture is not owned by any node (user/participant) or controlled by a single central authority. Many users have access to the data and have a copy of the blockchain database. Immutability: After data being validated and verified, it is stored and recorded in the blockchain. After recording data in the blockchain, it cannot be altered or modified which increase the integrity of data. This feature helps to detect and mitigate tampering, when malicious user attempt to alter data after it is being recorded the hash value of the block containing that data will be changed, and the user needs to recalculate the hash value of all the following blocks.

Table 1. Types of Blockchain Frameworks

Blockchain framework	**Owner**	**Access control for consensus**	**Shared write access**	**security**
Public	Shared/no single owner	All	All	Very high
Private	Consortium	Restricted	Controlled based on the user-role	Based on the validation of entities
Hybrid	Public blockchain hosting private network	Public and restricted	Controlled based on the user-role (customizable)	Very high

2.2 Blockchain Vulnerability

There are vulnerabilities related to public blockchain model, these vulnerabilities may affect blockchain-based frameworks depending on the network architecture [10] such as:

- 51% Attack [9][10]:
This vulnerability can be exploited when a node (each user is considered as node in the blockchain) controls 51% of the blockchain which means the user has the majority of transactions, this node can validate transactions to be stored in the blockchain and violates the immutability property.

- Syble Attack [10]:
Due to the absence of central authority to control and manage the blockchain, a malicious node can replicate itself by creating various copies of its node to pretend that different nodes are using the network which allow that node to control the blockchain. This attack can be prevented by selecting the appropriate consensus algorithm.

- Hard Forks: [10]
Some vulnerabilities are related to the code itself in the exited frameworks that are used to develop a blockchain-base systems such as Ethereum. Hard forks refer to the change of the rules or protocols of the blockchain, it happens when the code is updated, and some nodes use the updated version of the blockchain, and the others use the old version which provide a fork. This vulnerability enables the attacker to turn the invalid blocks into valid blocks and recorded to the blockchain. The Decentralized Autonomous Organization (DAO) that is a set of contracts in Ethereum was developed by hard forks. In May 2016, there was a security incident as a consequences of DAO vulnerability that caused a loss of $50 million worth of ether.

2.3 Blockchain in Land Administration

Blockchain technology has been introduced to be integrated to the land administration systems due the benefits provided by blockchain features to solve the security issues of the existing land administration systems. Land administration systems has two security issues: double-spending, and tampering [4]. Double spending: When a person sells the land multiple times to different people. This issue can be solved by using of tokenization mechanism that will be discussed in section 5. Tampering: The modification or altering land information records. Due to the ease of adopting blockchain technology to the existing system and the use of cryptography and the properties of blockchain as discussed in section 2.1, it can enhance the security and maintain the integrity of data and solve the exiting issues. According to some researchers blockchain technology is still in the early stages for such system. Most of the proposed solutions can successfully mitigate security issues, detect, and complicate unauthorized activities on the system, but to fully secure the system and prevent these security issues we may need to develop a full automation blockchain-based systems utilizing provided technologies by blockchain

ISSN: 3079-5354

such as tokenization mechanism. Tokenization mechanism refers to "the process of blockchain token (specifically, a security token) that digitally represents a real tradable asset" [11]. Tokenization in land administration system means that each land will be represented as a token in the blockchain, and the transfer of the ownership will be as token transaction from the seller to buyer, tokenization means that the validation and verification of this transaction will be through smart contracts without interfere of any parties (i.e., fully automated transaction), this mechanism solves most of the security issues in the existing systems. Since blockchain is in the early stages and transforming land administration systems to adopt blockchain technology is not mature enough in the current state to adopt most of the mechanisms provided by the blockchain technology, the automation of land administration is currently limited [3][12].

2.3.1 Case Study

Since 2016, some countries started pilot research's for land registry frameworks based on blockchain technology such as Dubai, Russia, United Kingdome, and. some countries adopted blockchain to prevent security issues such as double spending or to mainly secure and store transactions on blockchain Japan [13]. At this section we provide some use cases of countries have been successfully developed and launched blockchain- based land administration frameworks with different structures and technologies, as shown in Table 2 [7].

Table 2. Case Study of Countries Developed Blockchain-based Land Administration Systems

Country	Implementation	Technology Used
Georgia	Using the existing blockchain based land registry by National Agency Public Registry (NAPR) and developing timestamp layer to be added to the land records of NAPR. People can access their land records on the NAPR website and sell it, and they verify the buyer.	A research developed by Bitfury Group, NAPR, and the Blockchain Trust Accelerator.
Brazil	Using Bitcoin blockchain and hash records to prevent tampering.	Bitcoin (public blockchain)
Sweden	Maintain land records in Post Chain database to manage the blockchain.	Private permissioned blockchain
Estonia	The purpose of the blockchain it to manage changes of the data of lands in the e-Land register in the e-Court system.	Distributed Ledger Technology (DLT)
Ghana	Using public blockchain with role-based controls for users to provide transparency and tamper-proof system	Ethereum (public blockchain)

3. Research methodology

In this research, the mapping study was used. There are number of reasons of choosing this method. First, it is an effective way of identifying and evaluating the relevant studies with respect to research questions. Second, the mapping study is a well-defined way to synthesize and review the empirical evidence concerning a technology or method. Third, it provides researchers with the background knowledge to justify new research. Fourth, it provides researchers with the background knowledge to justify new research. The databases that were used to collect the papers: Saudi Digital Library, IEEE Explore, Google Scholar, ResearchGate, Springer, ArXiv and ScienceDirect. This section includes the PRISMA flow diagram to show the selection process Figure 1. The mapping study has been prepared, including the details of all steps. A brief description of the major steps as following:

1. Identifying the research questions
2. Identifying the search string and search process
3. Defining including and exclusion criteria
4. Mapping the data with research questions and data extractions
5. Result extraction and data

3.1 Search Strategy

The searching process started with the string "Blockchain for Land Records" in IEEE. The main reason of choosing IEEE is that it is famous well-known library contains vast collection of articles from different domains. The main searching string used was:

1. Blockchain-based land administration framework
2. Vulnerabilities in land administration and blockchain
3. Immutability of blockchain
4. Double spending and tampering in blockchain frameworks. These strings were considered in collecting all possible studies.

The searching result gives a lot of articles which cover blockchain-based land administration topic, the articles was useful to our study. For that, we decided to use it in the future for data extraction. The process data extraction theme that is used is shown in figure 2, and the word cloud of keywords and title of the research articles shown in figure 3 and figure 4, respectively

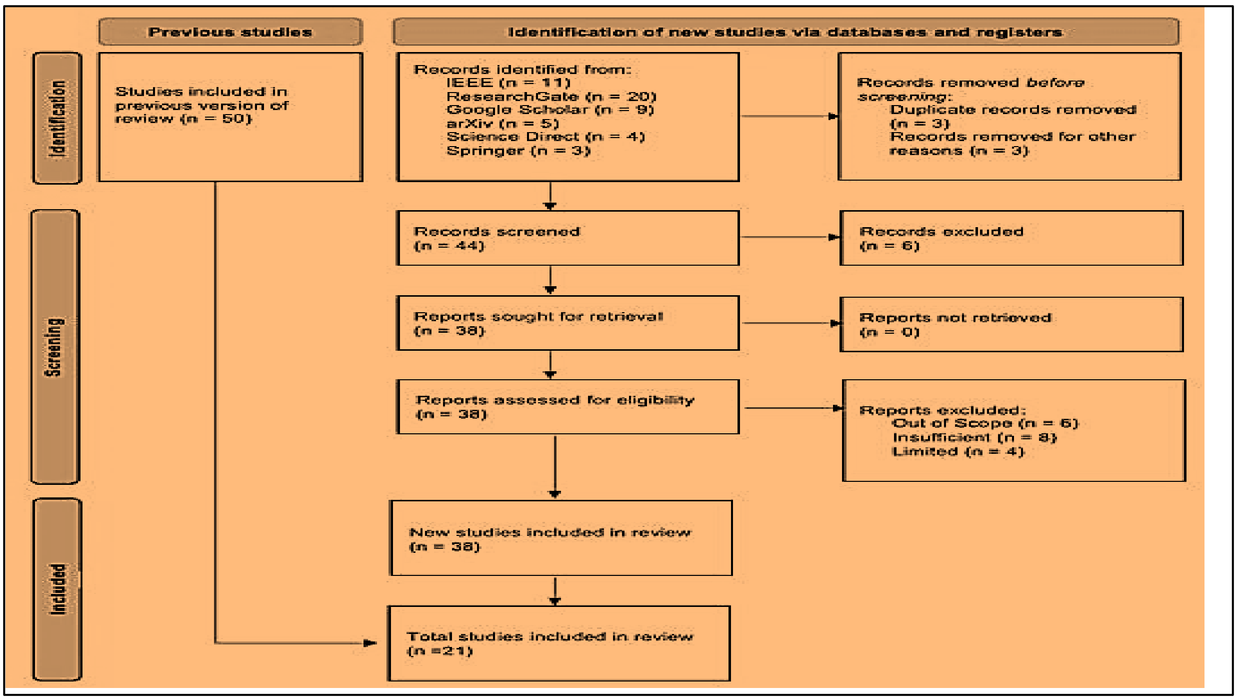


Figure 1. PRISMA Flow Diagram

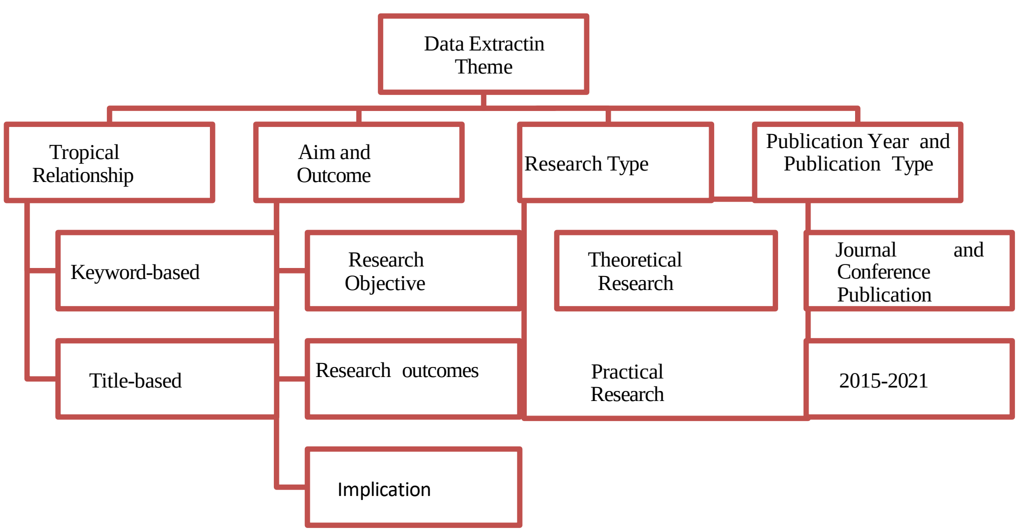


Figure 2. Data Extraction Theme

Figure 3. Word Cloud for Keywords of the Selected Research Papers

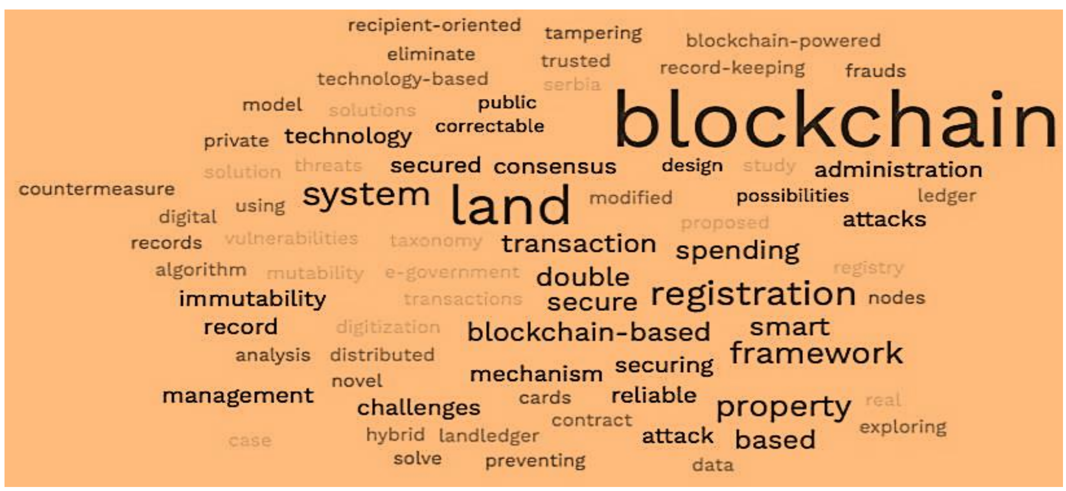


Figure 4. Word Cloud of the Titles of Selected Research Articles

3.2 Planning to Review

This sub-section provides the research questions to be answered through the research process. The objective of this systematic review is to examine existed land registry systems (included both traditional and digital), and analysis the vulnerabilities or flaws of the proposed frameworks and highlight the needed further work. The main research questions are formulated as following:

RQ: Can land records be represented as non-fungible tokens (NFT)?

4. Related Works

This section includes the systematic review of existed and proposed blockchain-based land administration frameworks, the summary of the analysis of related work is summarized in Table 3. Traditional land record systems have been in concern to be modernized and transformed centralized system to a decentralized distributed system to improve the procedures. Blockchain technology is known as a distributed ledger which offer a suitable solution to substitute the traditional land record systems regarding to its architecture which provides a secure environment for storing data and using cryptographic protocols. This article [5] highlights the benefits added to the land record systems by using blockchain technology, such as improving trust, and maintain integrity. While blockchain is newly applied to some applications and systems, this transformation may arise some concerns regarding to blockchain technology itself such as irreversibility, which may become as a disadvantage in some cases like fraudulent, errors of transactions. Another issue that is related to the blockchain infrastructure, it is designed to be free of single point of failure. This may lead to a problem in case of errors in transactions. The author also mentioned some practical researchs of blockchain-based land record systems that are implemented, and some are under development. Republic of Georgia is one of the first countries that develop and transform traditional land record system to blockchain-based system. A private permissioned blockchain architecture was used for the research administrated by a third part National Agency of Public Registry (NAPR). The research was successfully completed and showed result of increasing trust and transparency. The author concluded that the type of blockchain architecture used is critical, public blockchain is not suitable for the land record systems where it affects the main function of the system. According to the research results and implemented researchs blockchain improves the security of the transformed land record system but the selection of the architecture should be either private or hybrid (combination of public and private blockchain) architecture. Since the most type of blockchain used in the new or transformed systems is public, it might be challenging to effectively utilize the characteristics of blockchain such as flexibility, scalability and preserving security while enhancing and facilitating the provided services. Authors [14] highlights that how the advantages of blockchain become disadvantages in some cases. For example, blockchain is peer-to-peer which allows transactions without a third-party that is difficult to specify the responsibility in case of some problems. Also, the transparency in public blockchain means that transactions are traceable.

Another main advantage of blockchain is immutability, means that the transactions cannot be modified or deleted after storing in the blockchain to keep data protected and preserve integrity. This advantage can be turn to a downside of the blockchain technology in case of faulty transactions, this research [15] suggested a correctable public blockchain that preserve the advantages of blockchain but also enhances the scalability and flexibility of the public blockchain and keep data integrity even after correction. The proposed solution introduces a second blockchain that is linked to the original chain to store the correction data. This solution is practically applicable to the existed blockchains by extending them to be linked to a second chain. Since the original chain is extended it may rise risk of reducing security, but the proposed solution adds new functionality to maintain security. The evaluation of the proposed architecture shows that it decreases the throughput and doesn’t significantly increase the validation time of correctible blocks. The architecture is practically feasible.

Since blockchain is designed to be immutable or irreversible, Authors [16] show that blockchain cannot be fully immutable, in some cases blockchain records can be reversed, these blockchains can be described as tamper-evident structure where there is evidence of tampering as a result of cryptographic linked blocks. The length of blockchains is proportionally increasing its resilience, when an attacker or malicious user try to temper recorded data, it will change the hash pointer in the subsequent blocks and the recalculation of the hashes will be computationally expensive. Authors [16],[17], show that immutability and tampering-proof are affected by the majority of nodes and if the nodes belong to the same authority where they have the majority to agree and validate the change or adding to the blockchain. Thus, tampering seems to be rarely successful but not impossible, that should not be ignored.

Authors [1], classify blockchain as strong immutability under the condition that the protection of unauthorized or malicious modifications is provided by increasing the compositionality of a difficult problem. In permissioned blockchain, modification of a block in the chain could be considered as recreating all the blocks succeed that block and all the hashes of these blocks will be recalculated, a blockchain is also considered as immutable if the process of creating every block in the chain is hard. Immutability of blockchain is related to timestamping issues, authors presented a single-party cryptographic timestamping mechanism using proof-of-sequential-work (PoSW) that is a time-variable and can be applied to permissioned blockchain instead of Proof-of-Work (PoW) to ensure immutability. That adds an advantage to the blockchain by thwart modification of blockchain managed by one authority. The motivation of transforming land record system to blockchain-based system in some countries is to reduce cost which means reducing the processing time, the cost and providing a higher security environment for transactions.

This paper [18], authors analyze the Serbian land information system (LIS) and propose a system that can improve the existed system by using blockchain technology to enhance the security and benefit of the advantages of blockchain, the main concern is how to keep transactions secure. In this paper, transactions on blockchain are defined as “any kind of an event such as electronically signing a document or buying or selling property”, and to secure these transactions the system must be immutable and temper-proof. According to the research, some researchers find using blockchain in land administration considered as disadvantage since the technology has not been mature enough to be used in these sectors. Authors analyzed the existed Serbian land information system (LIS) which consists of two parts: cadastral record and cadastral map which identify the two types of data that is stored in blockchain alphanumeric and geospatial data. LIS has main privacy issue that data of transactions can be compromised either intentionally or unintentionally errors, it uses a centralized database with traditional web application. The proposed architecture is permissioned public blockchain on top of Ethereum, and it is still including some of traditional LIS components, but it uses a decentralized application (DApp) on

Ethereum to access the public blockchain and store transactions. Also, it uses Ethereum Virtual Machine (EVM) to use the smart contract and increase security. The proposed system isn't fully automated which needs further work to automate the transactions without any intermediate, but it increases the security and enhances the speed of transaction.

Authors [19], highlight the issues of the existed paper-based land registry system such as fraud, validation and verification, corruption, and time consuming. Authors proposed a blockchain-based system to store land records and it claimed as tamper-proof and reliable. The proposed framework consists of 11 steps, starting with pre-agreement which sign parties with unique id and the sell process. Then, sell request which is important step of the system where the system will lock the land title which means prevent any other transactions to access the locked sell id and this specifically designed to prevent double spending. The verification and approval are done by the registry office after validating the required information from the involved parties: seller, buyer, and the bank. Then it transfers the ownership and certify it, and the last step is to update the record in the blockchain using the hash for all parties in the system. The proposed framework reduces the time and provide reliable system. Authors [20] proposed a swarm-based framework that consists of three main steps stamp procurement, land ownership verification and record keeping. The system will connect all the registry offices, and validators will be connected as peer-to-peer through the network. The proposed system prevents unauthorized access by encrypting all the records data by the registry office's public key and store them on the network and must be decrypted with the registrar private key. Double spending is unlikely to occur but not impossible since when the request of a land sent to the e-registry system will reject any other request to the same e-registry.

This paper [21] indicated that each type of blockchain has its own characteristics which the combination of these characteristics is desirable and beneficial for some applications. This paper proposed a blockchain architecture that is hybrid blockchain (combination of public blockchain and private blockchain). The public blockchains is implemented on Ethereum and the private one is implemented in Amazon Web Service (AWS). The proposed framework shows that hybrid blockchain provides the transparency of public blockchain and the security of private blockchain. Authors [22], the main motivation of the proposed network is to improve security by prevent double spending and tampering. The proposed network is single main chain means that all blocks are linked with cryptographical hash and verifies transactions by Merkle tree. Each user on the network has a public key stored in the blockchain and the private key is only used by individual to sign into their platform. The network consists of 12 nodes, the verification is done by calculating Proof-of-Work (PoW). SHA-256 is used to encrypted transaction and calculating hash values that link the blocks. Tampering is prevented by the used PoW algorithm, when an unauthorized user attempts to modify the blockchain its private key is transferred to the network and sent to the other node to verify the public key which will fail.

Authors [23], proposed an automated record registration system, seller and buyer will register through the registry blockchain web application to verify their identity, land information, and transaction information, and the verification will be done through the government department. The authentication for signing into the system is done by Proof- of-Work (PoW). Smart contract is used to sell the land and provide a digital agreement that include all the sale details, and all documents will be signed digitally. The proposed system preserves data integrity by using tokens with limited time to verify and authenticate the documents. Authors [24] proposed a framework for land record system, the proposed framework is considered the updating of land information and checking land information as main functionalities of the land administration system. The proposed framework is implemented on Ethereum and uses Proof-of-Work algorithm for verification. The proposed system provides a robust and secure environment for land administration system by ensuring that only valid blocks are added to the blockchain by using consensus algorithm, also it is a tamper-proof where any changes in the chain will be detected immediately.

Authors [25] presented a blockchain-based system called LandLedger, the system is implemented on permissioned blockchain. It uses Merkle Patricia Tree to verify the ownership. The architecture consists of 4 phases' initialization, verification, registration, and revocation. LandLedger ensures the most important concerns which are immutability, prevent double spending, and tampering-proof. The system preserve immutability by using SHA256 for hash function and digital signature. Also, it prevents double spending where the property has a unique id and cannot be requested for more than one transaction. Authors [26] proposed novel framework that enhances the security, increase speed, transparency and prevent tampering. The system is swarm-based network, peer-two-peer architecture implemented on top of Interplanetary File System (IPFS). The reason behind selecting IPFS platform is that it offers functionality, decentralization, and provided flexibility to the developers. The framework consists of 6 entities that participated in the system: government-owned land registry office, region, web server, registry office miner, authorized professional miner, and bootstrap server. The proposed system uses Trusted Nodes Consensus Algorithm (TNCA) instead of Proof-of-Work (PoW) to reduce the time of processing and the number of exchanged messages. The system showed great performance, but it doesn't provide a special mechanism

to prevent tampering, double spending, or increasing immutability. The registration is done by submitting documents includes map, ID proofs, and two witness to the sub registrar office to verify and sends them to the government-owned land registry office which is not automated and rely on trust of individuals.
Authors [27] proposed a system that uses blockchain and Interplanetary File System (IPFS), the data will be stored in the IPFS to prevent tampering and the hash address produced by the IPFS will be stored in the blockchain. This framework enhances the security of data and increases reliability. They stored data on IPFS because of the immutability of the blockchain. The system also uses a local database management system to trace public user details and transaction hash code. Another feature is added to the smart contract that is the hash address is of the previous owner is stored to allow trace information of the land. The proposed system increases the speed and provide a reliable security.

Authors [28] showed that double spending may occurred by a malicious miner that has a strong computational power that enables the miner to select transactions, add, and verify them faster to the miner's isolated blockchain. This paper [29], proposed a solution for preventing double spending. The proposed method is that every transaction can be completed successfully only when the recipient confirms the validity of transaction within a fixed waiting duration. This research [30] proposed a secure system for storing records using hybrid blockchain. In the proposed system only members of the blockchain are allowed to view the data and others are allowed to view the properties that offered for sale. The system provided reliability and access control. There is no mechanism to prevent double spending in the proposed system, but it prevents passive attacks by unauthorized users. Authors [31] proposed a multistage secure pool framework to prevent double spending at analytical layer and implementation layer, the framework involved of 4 phases: detection, confirmation, forwarding, and broadcasting. Each stage is responsible to provide a specific characteristic, detection stage is the security obstacle of double spending where detection parameters are used to detect anomalies in the system such as match a transaction stored in the blockchain. The system will provide a one-time sweep of the network looking for any duplication in transactions. In the confirmation stage the miners must determine the level of confirmation they needed to process a transaction. In the third stage, the data is forward to the network for approval. In the last stage, private data will be broadcasted to the system to aware the miners in case of attacker activity is detected in the network. Author [32] proposed a Blockchain based Secure Smart Property Registration Management System (SSPRMS), which is tamper proof and provide permanent storge for the land. The system uses Hyperledger as public blockchain, the proposed system provides rapid ownership transformation, eliminates the interfere of third parties. The system also proposed the use of Smart Property Card (SPC) which utilize a mechanism to store property information and the update state on the smart card instead of the documents. Also, it allows to transfer funds digitally from buyer to seller.

Table 3. Summary of Systematic Review of Related Work

Reference	Objective	Problem statement	Used mechanism	Result/Limitation proposed framework
[5]	Highlights the importance and benefits of digitizing traditional system using blockchain technology and the challenges of blockchain adoption	Utilizing blockchain to mitigate fraudulent and maintain data integrity in land registration system	Private blockchain in republic of Georgia to develop blockchain-based land registry framework	The framework has been developed successfully and increased trustand transparency
[14]	Highlights how the public blockchain advantages may turn to challenges in the use of public services systems	The difficulty of determining the responsible party in case of transaction errors in public blockchain	Public blockchain	Public blockchain provides flexibility, scalability but it might be challenging for transaction security

[15]	Proposed correctabe blockchain to avoid faulty transactions while maintain immutability of the blockchain	Immutability of blockchain can be a disadvantage in case of faulty transactions	Proposed a correctable architecture that adds a functionality layer the existed blockchain that uses second blockchain that is extended and linked to the original blockchain	The architecture reduces the throughput but does not increase the validation time, and it is practically applicable
[16]	Shows the level of immutability in blockchain	Blockchain cannot be fully immutable, in some cases records in the blockchains can be reversed	Cryptographic functions to avoid tampering	The length of blockchains can proportionally increasing its resilience by detecting the changes inf hash pointers in the subsequent blocks
[16][17]	Shows that blockchain properties: immutability and tamper-proof can be affected by the nodes in the network	In some blockchain network, the majority of nodes belong to one authority can agree to validate unauthorized transaction	The nature of blockchain technology can prevent this type of malicious transactions	this issue should not be neglected and rely on the blockchain properties
[1]	Shows the conditions that enables the blockchain to be classified as strongly immutable	Increasing the immutability by increasing the complexity if validation problems	Presented single-party cryptographic mechanism using proof-of-sequential-work (PoSW)	This adds an advantage to blockchain by thwart the vulnerability of unauthorized modification by majority of nodes
[18]	Proposed a system that is using blockchain and enhancing security of existing land record systems and utilizing blockchain properties	Transform existed systems to immutable and tamper-proof system	Proposed permissioned public blockchain on top of Ethereum integrated with existed traditional land administration components	The proposed system is not fully automated and need further work to automate transactions without interfere of intermediary
[19]	Highlights the issues of the existed paper-based land registry system	Security issues of traditional land registry systems such as fraud, verification and validatin, corruption	Proposed blockchain-based system to store land records to provide tamper-proof system	The proposed system provide a reliable land administration system
[20]	Provides framework to mitigate security issues such as double spending	Unauthorized access to the land records	Proposed a swarm-based framework that is connected to the registry office	Prevents unauthorized access to records by encrypting all the records using the registry office's public key, but it cannot fully prevent double spending

[21]	Highlights the various advantages of each blockchain type	Utilize the benefits of public and private blockchains	Proposed a hybrid blockchain architecture. The public blockchain is implemented on Ethereum and the private blockchain is implemented on Amazon Web Service (AWS)	The proposed architecture shows that it can utilize the transparency of public blockchain and the security of the private blockchain
[22]	The main motivation is to improve security, and prevent double spending and tampering	Double spending and tampering in the existed systems	Proposed a network that is single main chain linked with cryptographical hash and verifies using Merkle Tree	Prevents tampering and unauthorized modification by using proof-of-work (PoW) algorithm
[23]	Proposed an automated record registration system	Provide blockchain-based automated framework to overcome security issues	Buyer and seller will register to blockchain web application to verify identity, and land information,	Proposed system maintains data integrity by using tokens limited with time to verify documents
[24]	Proposed a framework for land record system for updating and checking land information	Ensuring that only valid blocks are recorded	The proposed framework is implemented on Ethereum using proof-of-work (PoW) algorithm for verification	The proposed system shows tamper-proof results and detects una uthorized modifications
[25]	Presented blockchain-based system called LandLedger	Verify the ownership of lands	Proposed permission ed blockchain using Merkle Tree to verify the ownership	The system preserves immutability and prevents double spending by generating unique ID foe each land
[26]	Proposed novel framework that enhances security, increases transparency, and prevent tampering	Tampering in the existed frameworks	Proposed a swarm-based network, P2P network on top of Interplanetary File System (IPFS). It uses Trusted Nodes Consensus Algorit hm (TNCA)	The system shows great performance but it does not provide a special mechanisms to prevent tampering, double spending, or increase immutability
[27]	Proposed a system that uses blockchain and Interplanetary File System (IPFS) to store the data in the IPFS to prevent tampering	Overcome tampering in land record systems	Store data in IPFS and store the hash address produced by IPFS in the blockchains	The framework enhances security, increases reliability. Also, allows to trace information of the land
[28]	Shows that double spend can occur by nodes with major computational power may be able	Double spending as a consequence of nodes with computational power	Minors with computational power can add or modify transactions faster than other minors	No framework was proposed
[29]	Proposed solution to prevent double spending	Double spending in land systems	Propose a method in which every transaction must be verified and confirmed by the recipient within a fixed waiting duration	It would not work in case of the transaction was sent to multiple nodes with different time durations

[30]	Proposed a secure system for storing records using hybrid blockchain	Preventing unauthorized access	Only members of the network will access and view data, and the public can only view lands for sale	No mechanisms to prevent double spending, it prevents passive attacks by unauthorized users
[31]	Proposed a multistage secure pool framework to prevent double spending at analytical layer and implementation layer	Double spendi ng issue	The framework involved of 4 phases: detecti on, confirmation, forwarding, and broadcasting. Each stage is responsible to provide a specific function	It provides detection function against double spending
[32]	Proposed a Blockchain based Secure Smart Property Registration Management System (SSPRMS), also it proposed the use of Smart Property Card (SPC)	Tempering a nd double spending	The system uses Hyperledger as public blockchain, and Smart Property Card (SPC) which utilize a mechanism to store property information and the update state on the smart card instead of the documents	The proposed system provides rapid ownership transformation, eliminates the interfere of third parties, and allows to transfer funds digitally from buyer to seller

5. Proposed Framework

There are factors that important to affect the main objective of the framework, which are the type of blockchain and the type of platform. There are several of platforms to develop and build blockchain-based frameworks such as Ethereum, Bitcoin, and Hyperledger. For this research we selected Hyperledger framework to develop our proposed system. Hyperledger is an open-source collaborative effort of blockchain by Linux Foundation [33]. Ethereum and Bitcoin are public blockchain platforms, through the research and analysis of existed or proposed frameworks public blockchain has its own threats and each platform has its own weaknesses for such a system and does not provide effective solution to our main concerns: double spending and tampering. For our proposed system, we considered private blockchain model to be developed using Hyperledger research. The vulnerabilities in section 2.2 cannot be exploited in private blockchain since the transactions will be decided and validated by government authority and nodes will not belong to a central authority and join to form majority of nodes. Also, the mitigation of double spending and immutability of the system will be inherited by the private blockchain.

5.1 Hyperledger platform provide various distributed ledger technology (DLT) frameworks and tools to be used for blockchain-based frameworks and related application. Some of these frameworks are public, private, or support both structures. Both frameworks and tools are listed below [33]:

1. Hyperledger Frameworks:

- Hyperledger Burrow
- Hyperledger Besu
- Hyperledger Fabric
- Hyperledger Indy
- Hyperledger Iroha
- Hyperledger Sawtooth

For our research we will use Hyperledger Fabric, it is an intended framework that allow to develop blockchain-based application or solution for wide-range use cases. It is private blockchain, it supports consensus protocols and membership services. Also, it provides unique approaches to preserve privacy.

1. Tools:

Hyperledger provides multiple tools to facilitate the development of blockchain-based frameworks and applications, we will use a combination of the listed tools in the implementation of this research:

- Hyperledger Avalon: It is a ledger independent implementation by Ethereum Alliance, it enables developers to gain computational trust.
- Hyperledger Bevel: Helps developers to deploy secure, scalable, and production ready DLT networks.
- Hyperledger Cactus: Allows users to integrate multiple blockchains in a secure manner.
- Hyperledger Caliper: Allows users to measure the performance of the implementation.
- Hyperledger Cello: Facilitates creating, managing, and terminating blockchains
- Hyperledger Explorer: A tool used to view, invoke, deploy, or query blocks, transactions, and data.
- Hyperledger Firefly: A multiparty system allows developers to rapidly build blockchain apps for enterprise.

5.2 *Hyperledger Fabric*

Fabric is a platform for permissioned blockchains that developed for distributed applications. Fabric supports different programming languages for applications such as Go, Java, Node.js. Hyperledger Fabric provides permissioned network that is managed as consortium network, and transaction security which solves the main issues of land administration systems. Also, it offers tokenization mechanisms by Fabric Token SDK, which solves the problem of double spending. Tokenization in Fabric, allows to represent any type of assets to tokens, allows to determine the privacy level in adoption to the use of system, and audits transaction of tokens. Hyperledger Fabric consists of major components that are listed in the following:

1. Peers:
Peers execute consensus protocol to validate transactions, there are three types of peers in Fabric:

- Endorsing Peers: Receives transaction proposal from the client that is executed by the smart contracts.
- Validators Peers: Validates transaction against endorsement policy.
- Committing Peers: Commit the transaction and maintain the state of ledger.
- Ordering Peers: receives the endorsed transaction, order the transaction into blocks, and distributed for validation peers to be validated.

2. Ledger:
Is a key component in Hyperledger Fabric, it stores information about objects; both the current value of the attributes of the objects, and the history of transactions that resulted in these current values.

3. *Membership service provider (MSP):*
In private blockchain, each node must be authenticated and has its own identity. MSP in Fabric provides certificates to the participant's nodes and peers in the network. It uses certificate authority (CA) to issue and verify certificates as following:

- Define the permissions for the nodes on the channel: local MSP for each node (clients, peers, orders), and channel MSP to define the administrative level and rights on the channel to authorize members.

- MSP will issue a private and public key and certificates for each node based on the definitions on local and channel MSPs

4. Organizations:
A group of peers that belongs to an organization, each organization has its own MSP to manage the identity of its peers.

5. Channels:
Allows peers belongs to an organization and application to communicate within the network.

6. Ordering Service:

A group of orderer nodes that broadcasts endorsed transaction to the validating peers. Fabric supports three types of ordering service, which are SOLO, KAFKA, and RAFT. Raft ordering service consists of three phases:

- Proposal: the client application will send transaction proposal to peers the chaincode.
- Ordering: if the transaction is endorsed, the client application will send the response of the endorsement to the ordering service. The transaction will be ordered and packaged.
- Validation and commit: validator peers will validate the transaction blocks and commit the transaction to be chained to the blockchain.

7. Smart Contracts:

In fabric it is called chaincode, it is a piece of program that is installed on every peer node to be able to access the network. It is written in high-level languages that is supported by Fabric such as Go, Java, Node.js.

5.2.1 Consensus in Hyperledger Fabric

Hyperledger fabric uses Raft protocol which is a CFT-based consensus algorithm, which is reach the consensus through the ordering service with the architecture execute-order- validate. Fabric introduces different transaction than the standard execution design, it uses execute-order-validate architecture to execute transaction through consensus protocol, and the flow of transaction through consensus protocol in Hyperledger Fabric is shown in figure 5. This architecture divided the transaction into three phases [34]:

1. Execution Phase: Clients send transaction proposal to endorsers to be executed and to check its correctness.
2. Ordering Phase: Submit transactions to ordering service through consensus protocol.
3. Validation Phase: Transaction validation against the endorsement policy, then it is appended to the blockchains and committed.

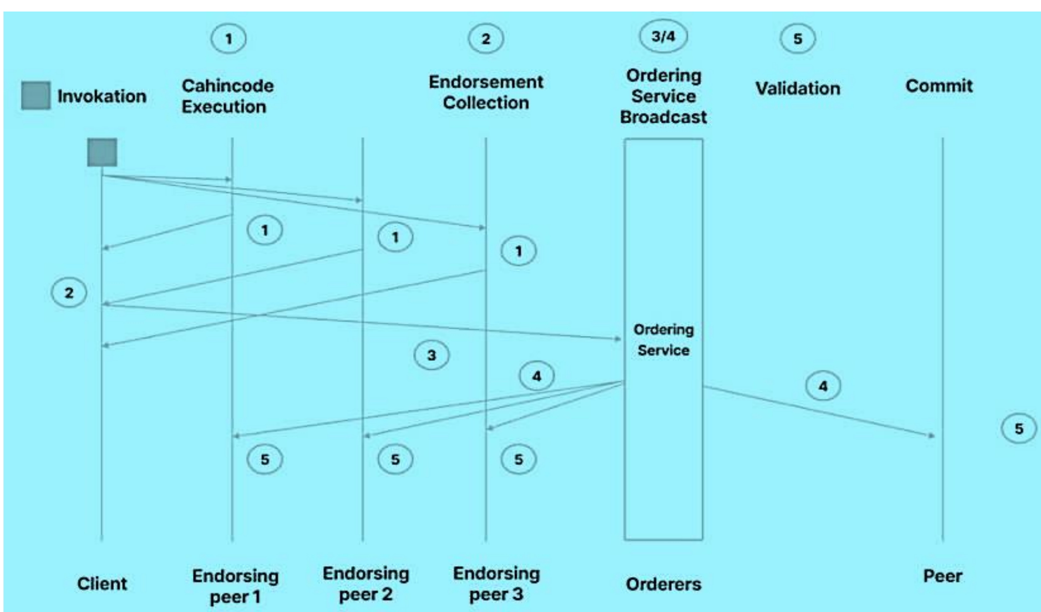


Figure 5. High Transaction Flow in Hyperledger Fabric

5.3 Proposed Framework

Our proposed framework will be private blockchain developed on Hyperledger Fabric, which will present land records as non-fungible tokens (NFT). The main tasks of our framework are user registration, land registration, and land transaction. The framework will use consensus protocol through ordering service architecture and sha-256 for hash function. The initial design of our framework is shown in figure 6, the nodes and transaction will be authorized and authenticated by the

 ISSN: 3079-5354

government authority which will issue certificates and verify transactions. Each node will have the chaincode installed on its machine, and all nodes will communicate to the network through a channel with sdk layer.

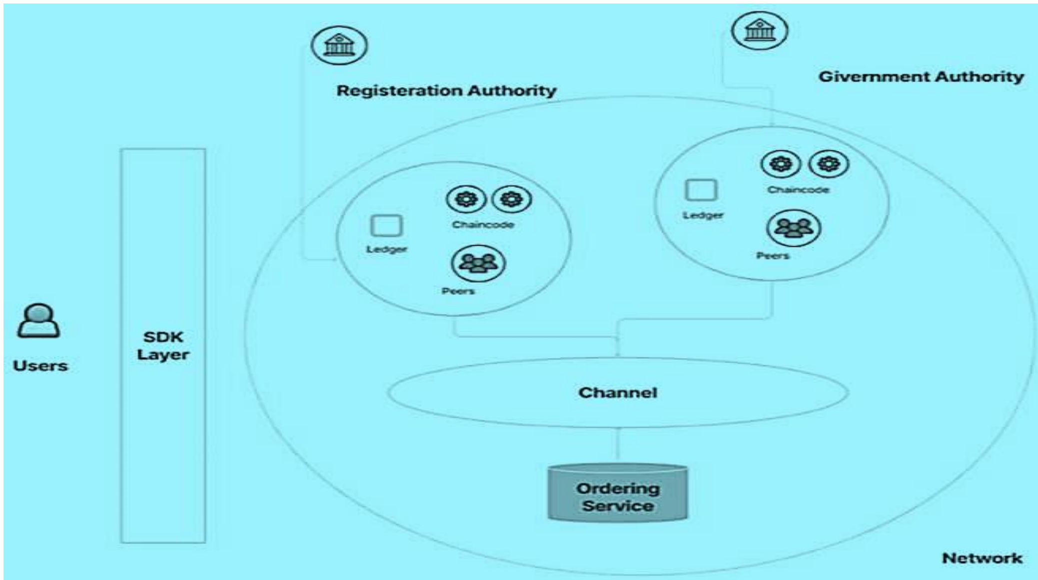


Figure 6. The Initial Design of the Proposed Framework

The main actors of the system are users (seller and buyer), registration authority, and government authority. The use case diagram in figure 7 shows the activities of each actor in the framework. In the following we will describe the flow of each task.

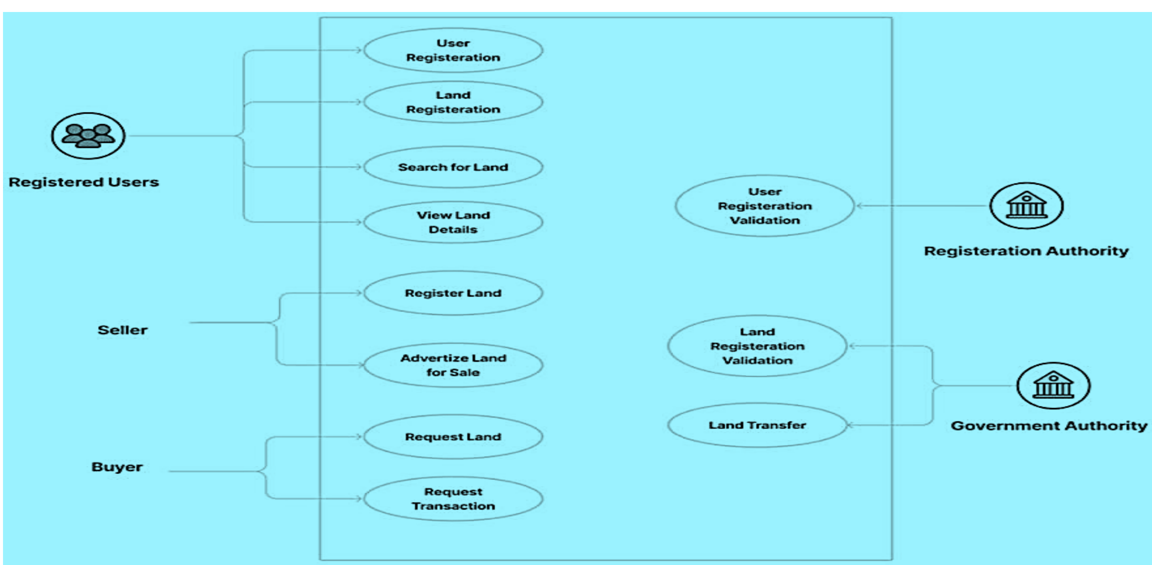


Figure 7. Use Case Diagram of the Proposed Framework.

5.3.1 User Registration

Seller and buyer must be registered on the system using national ID to be the unique identity of the user to be able to gain access and must be authorized by the government authority. The process of user registration is shown in the flow diagram in figure 8. The user must provide his or her information and the information will be validated of the government authority, and user account will be verified through registration authority (act as Absher). If the entered national ID is invalid the registration will be rejected, in case of valid information the user will be authorized and gain access to the system. The reason of using national ID as a unique identity of each user will reduce the effort of issuing a unique identity of each user and allow to trace the activity of the users. Then, compute hash using user attributes and signed by the government authority to be added to blockchain in an encrypted form.

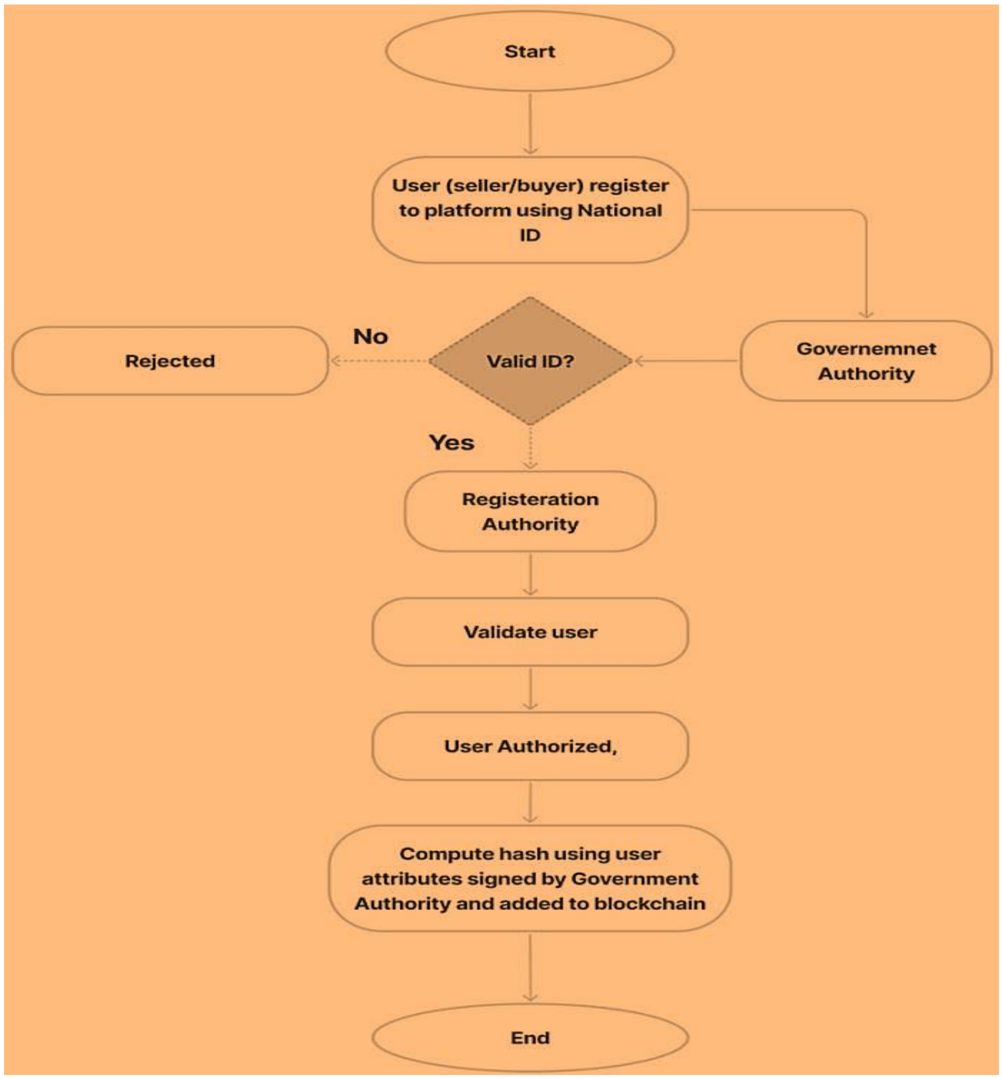


Figure 8. Flow Diagram of User Registration

5.3.2 Land Registration

The second task of our implementation is land registration, after the users have been successfully registered and authorized, they can add their own lands to the system as the following steps as shown in figure 9:

1. Users log in to the system.
2. Register their land by providing land information.
3. Government authority will validate the information and the ownership of the land, if information is authorized the land will be validated an added to the system.
4. Tokenize or generate unique ID to represent the land on the system to avoid double spending issue, compute hash using land attributes to store it and signed by the government authority.
5. Land will be added to record.

ISSN: 3079-5354

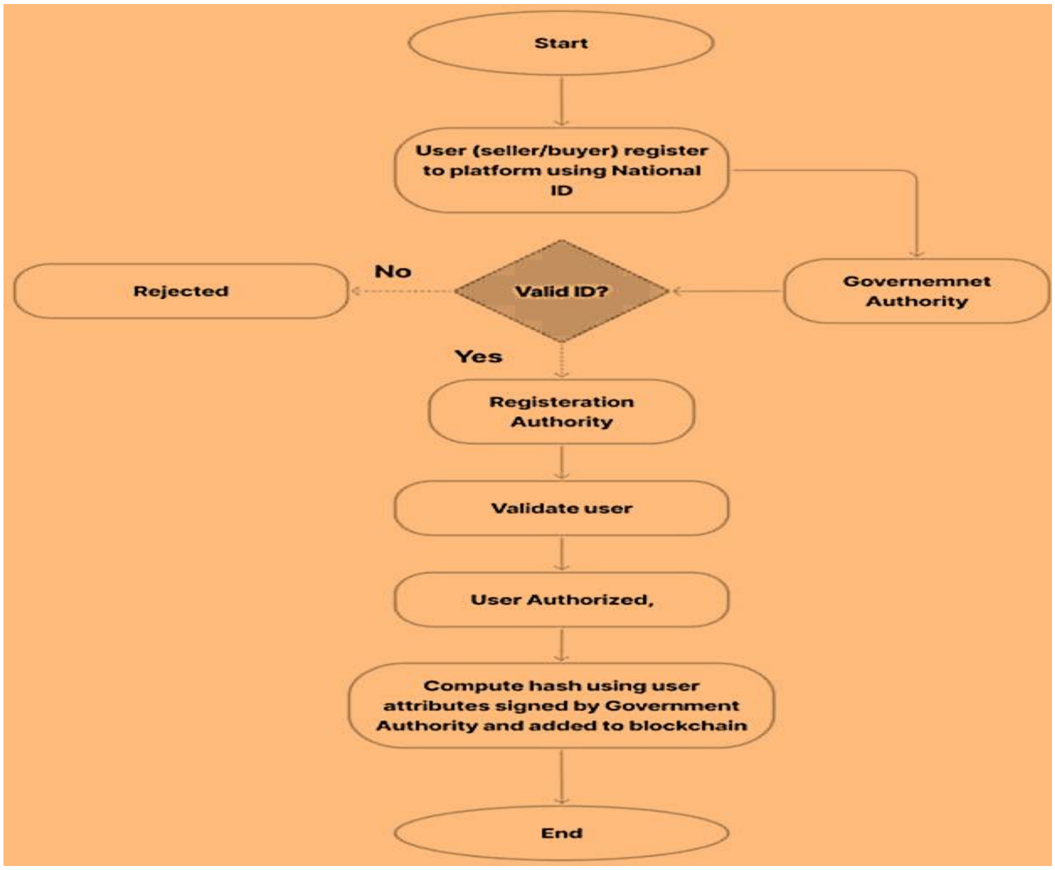


Figure 9. Land Registration to the System

5.3.3 Land Transaction Request

At this task, users can advertise their lands for sale and other users can search or view advertised lands. For this task we will integrate Hyperledger explorer to view lands. The process is shown in figure 10, as the following steps:

1. Users log in to the system.
2. Search or view advertised lands
3. Request land if the seller agrees then buyer will request transaction.
4. Transaction will be validated by the government authority through ordering service as the following, the transaction flow is shown in figure 11:

- Government authority initiates transferring land request to chaincode.
- Chaincode validates access and initial documents verified.
- Initiate chaincode if transferring land to endorsers.
- After validation, the transferring will be sent to the orderer to execute consensus protocol.
- Chaincode will return an acknowledgement to government authority and validate transaction and add it to the ledger.

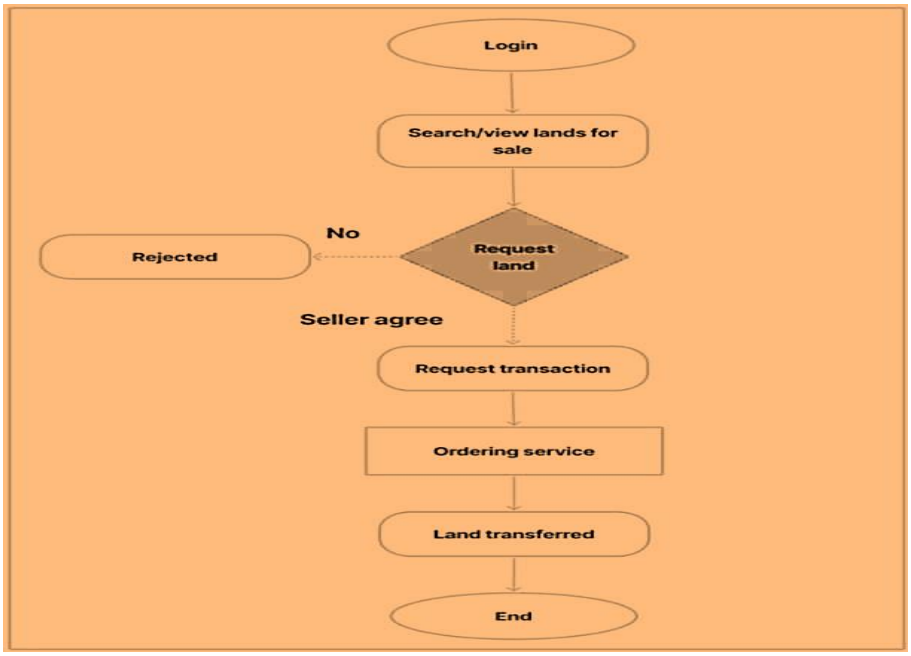


Figure 10. Land Transaction Request

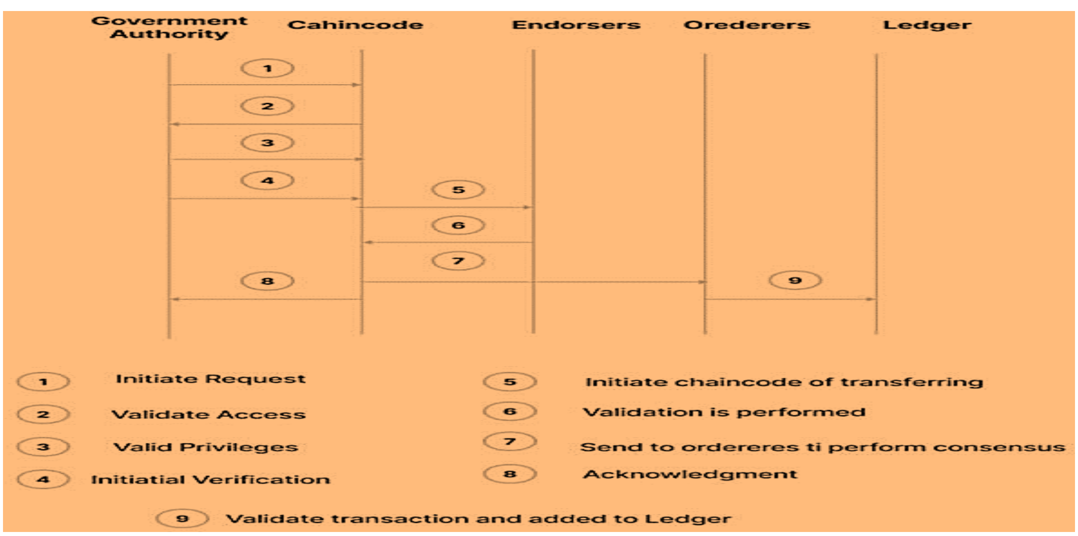


Figure 11. Transaction Request Flow

6. Implementation

This section includes the implementation of this research and technical details of the environment and specifications. The implementation of this research will be divided into two steps: deploying the network and deploying the chaincodes (smart contracts) and client API.

6.1 Implementation Environment

We select Hyperledger Fabric platform to implement our blockchain network on it, for the purpose of this research we used Hyperledger Fabric 1.1.0. The operating system is Ubuntu 20.4.0

*Setting Up The environment***:**
Before starting to use Hyperledger Fabric and building out network, Hyperledger Fabric has pre-Requests to install tools and software used to run the Hyperledger Fabric[12], the compatibility of requested software and the Hyperledger Fabric version and other tools is critical condition. The requested software and versions used to set up are listed as following: cUrl v7.68.0 Docker, v20.10.12, Docker-compose v1.13.0, Npm v6.13, 4, Nvm v0.33.2, Node.js.v8.17.0 and Go.v1.17.6.

6.2 Installing Hyperledger Fabric:

After setting the environment and downloading all the requested software, we need to install the Hyperledger Fabric tools to run and start the Hyperledger Fabric[3]. We installed all the components with version 0.19, the Hyperledger Fabric components are listed below: **CLI Tools:** Which provides all the essential operations for the rest of the components REST Server: A server that will be installed on the OS to be able to use RESTful APIs to interact between the client API and the network. *Hyperledger Composer***:** A utility used to generate the assets for application. *Yeoman:* It is a generator to run Hyperledger generator to deploy the application and the network. *Composer Playground***:** Online browser app to edit, test, and deploy the network.
All these components must be installed with same version and ensure the compatibility of these components with the pre-requested software mentioned in earlier. One of the issues of the setting of our environment that was the incompatibility of Yeoman generator with npm, node.js, nvm, and Hyperledger composer. Which solved by downgrading the Yeoman generator to older version.

6.3 Deploying Network

After successful installation of the tools and components, we start to create our network either using composer playground or the terminal. There are useful fabric samples for the networks to facilitate selecting the model of the network and its definition. Before start creating the network, we installed the Hyperledger Fabric by downloading Hyperledger Fabric v1.1 and using fabric scripts to start the Hyperledger Fabric locally. An important step is to start the Hyperledger script startFabric.sh file and create admin card to be used for network, as shown in figure 12, 13, 14.

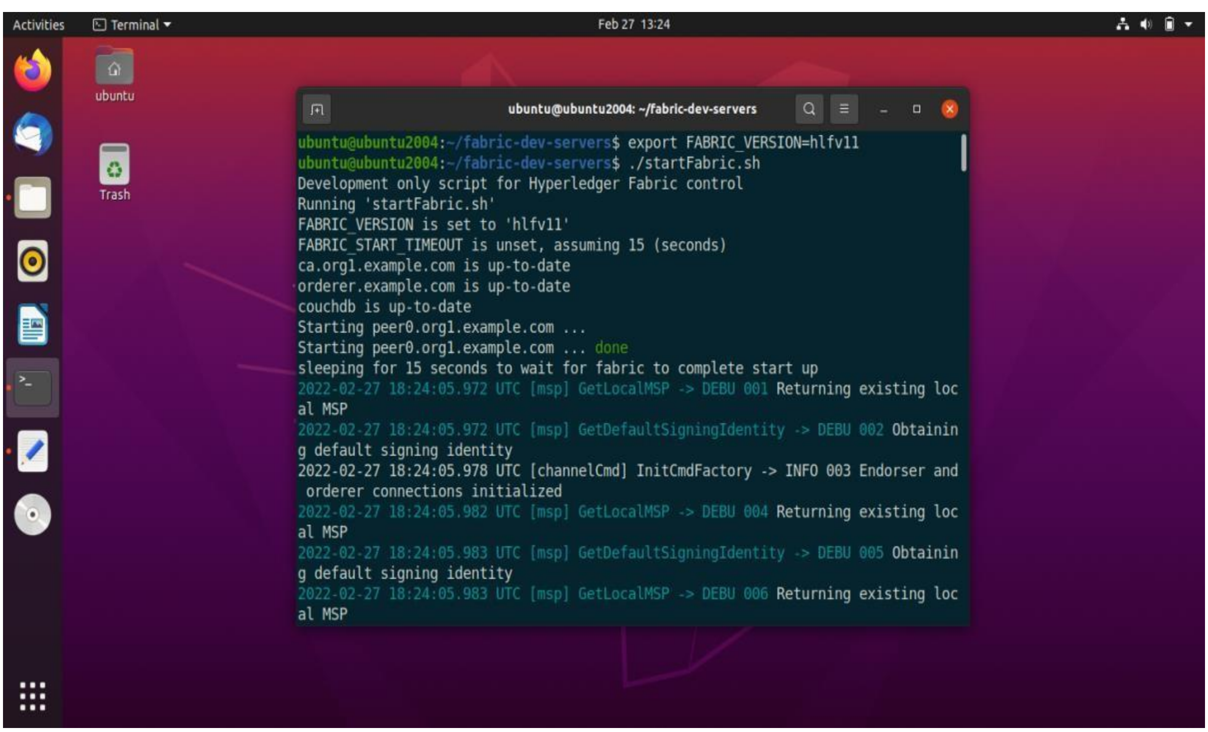


Figure 12. Starting Hyperledger Fabric and create docker images

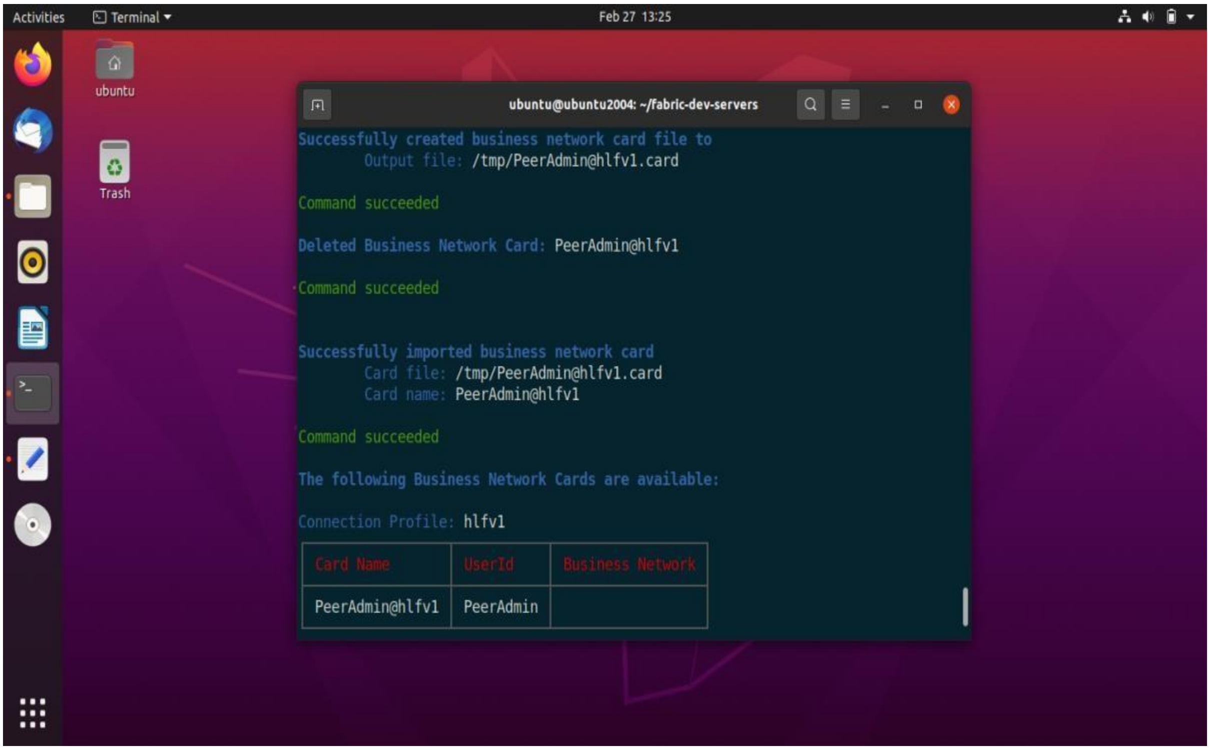


Figure 13. Creating admin card for the network

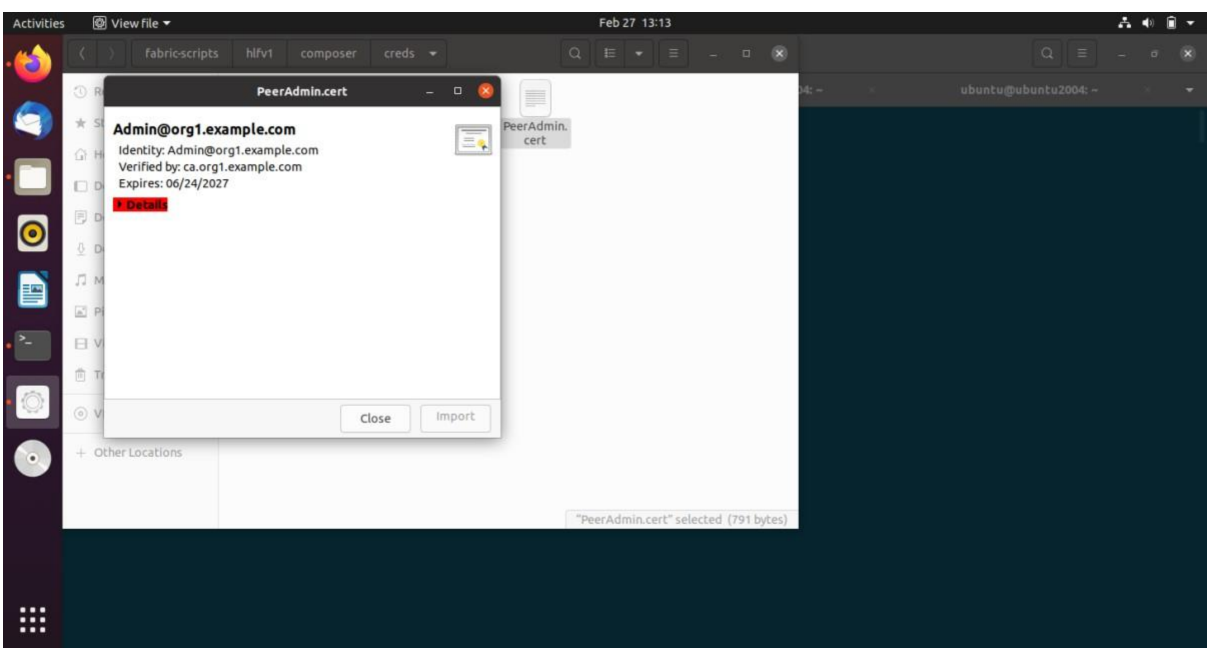


Figure 14. Admin certification after generating the card

The steps of deploying the network are as followed:

Step1: Create the network structure using Yeoman generator

At this step we generate the model structure, access controls, and the definition of the network as shown in the figure 15.

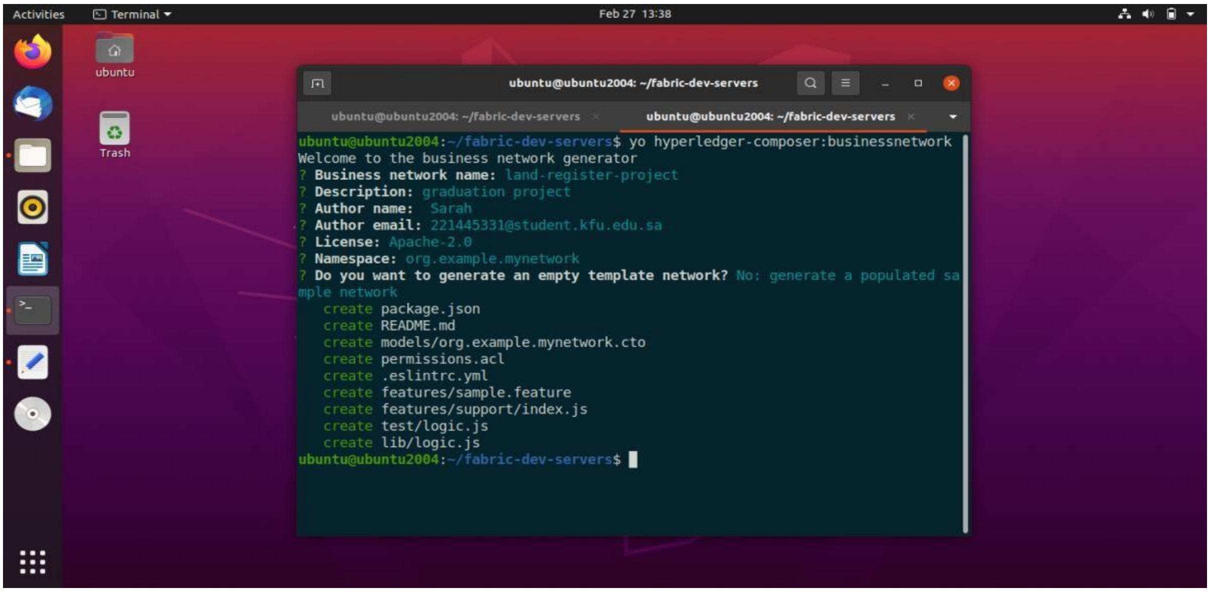


Figure 15. Creating the network by Yeoman generator

Step 2: Defining the network: At this step we set up the model file of the network org.example.mynetwork.cto, Hyperledger Fabric provides object-oriented modelling language to either define the structure of the network with new structure or use one of the built-in defined structures in Fabric. Also, we edited the logic.js file which is used for transaction logic.

Step 3: Generate Business network archive: This step is important to package out our network to be in a deployable form to run, as shown in figure 16.

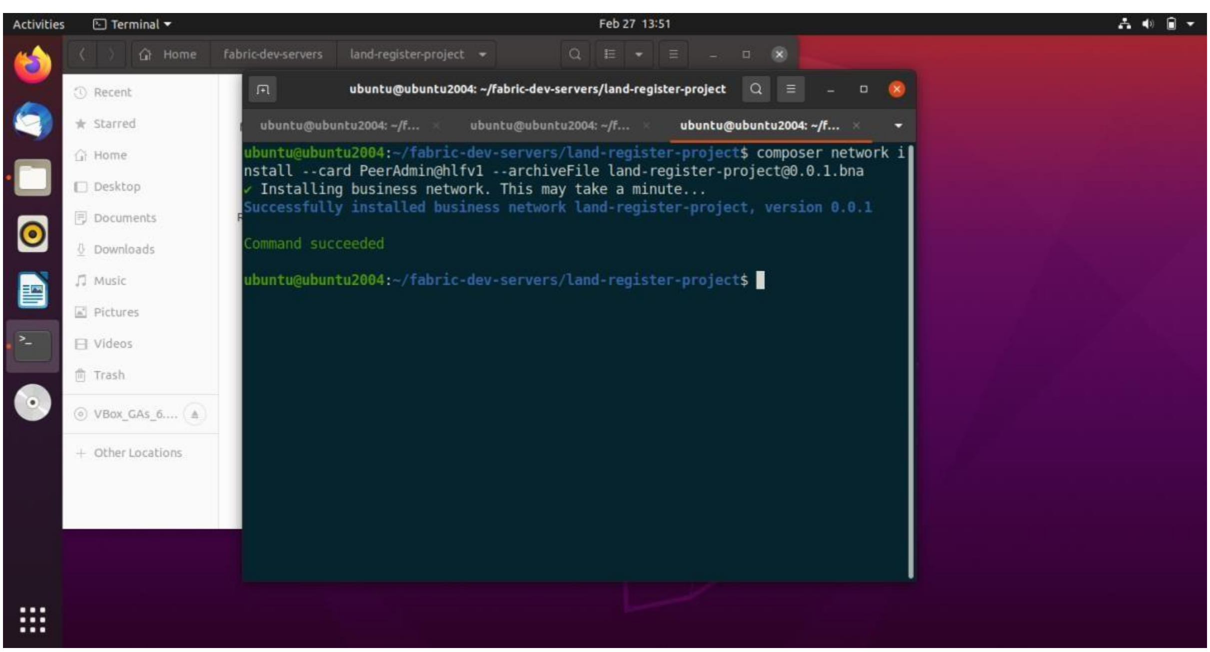


Figure 16. Generate the .bna archive file for the network

Step 4: Deploying Network: At this step, the network is deployed using composer network and run through the terminal and proceed to generate the REST API.

6.3.1 Testing the Network Using Composer Playground

After all the steps of initializing our network, we tested it on composer playground and test a simple transaction using trade asset. Figure 17, 18 show alternatively the added participants, where the sample asset is transferred successfully, and the owner has been changed. Figure 19 shows how the asset is successfully transferred to the new owner which became Trade 3 instead of TRADER1.

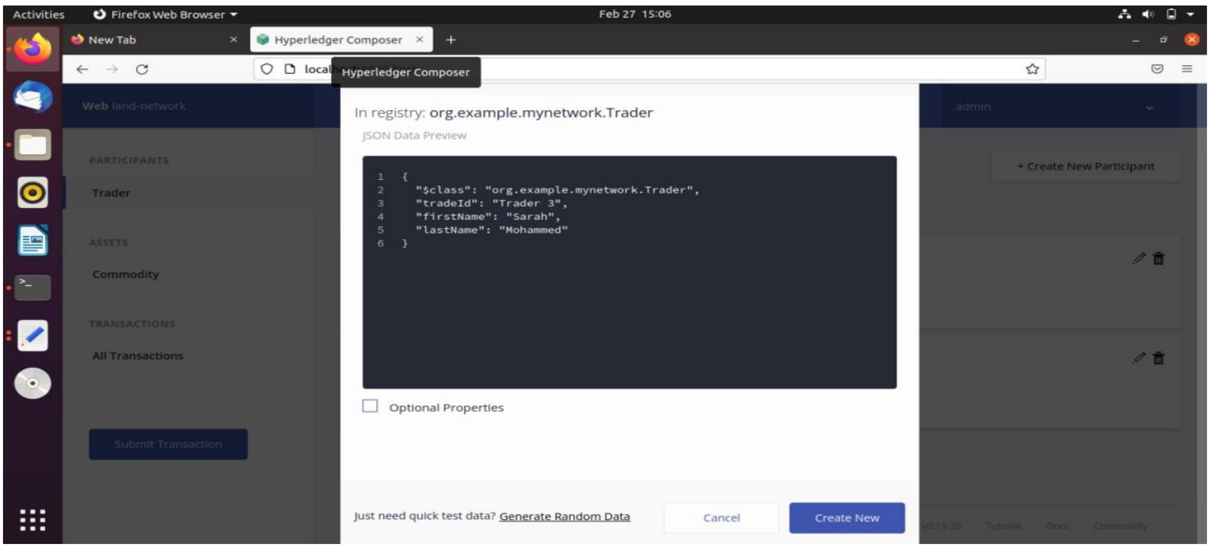


Figure 17. Adding new participant to the network

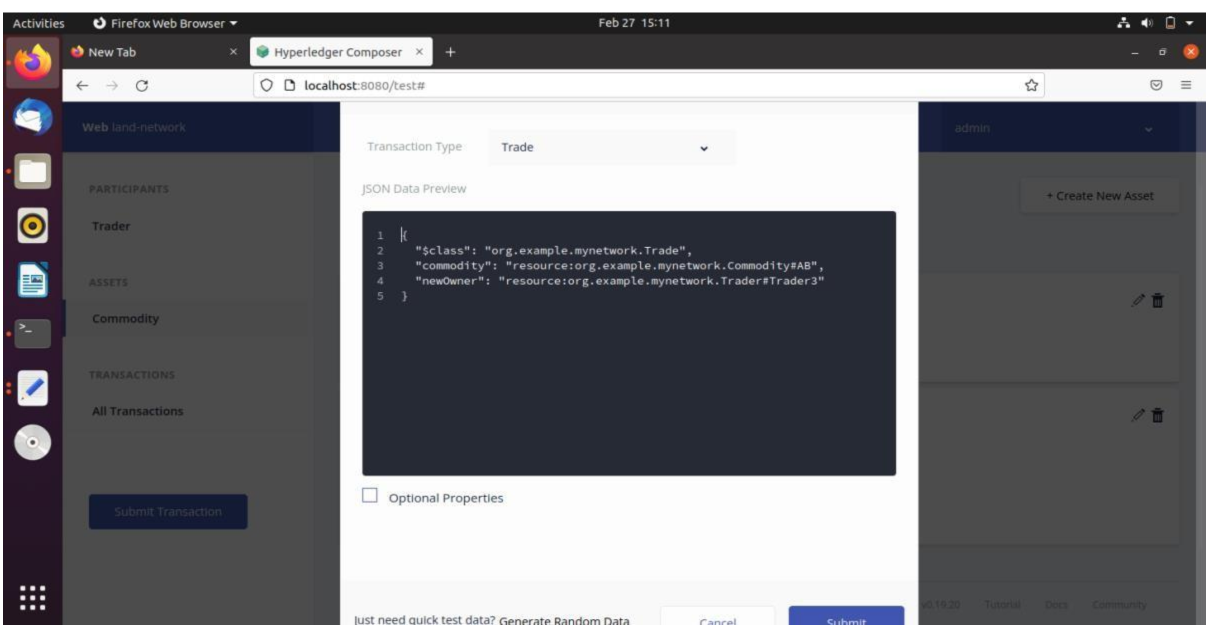


Figure 18. Submit test transaction

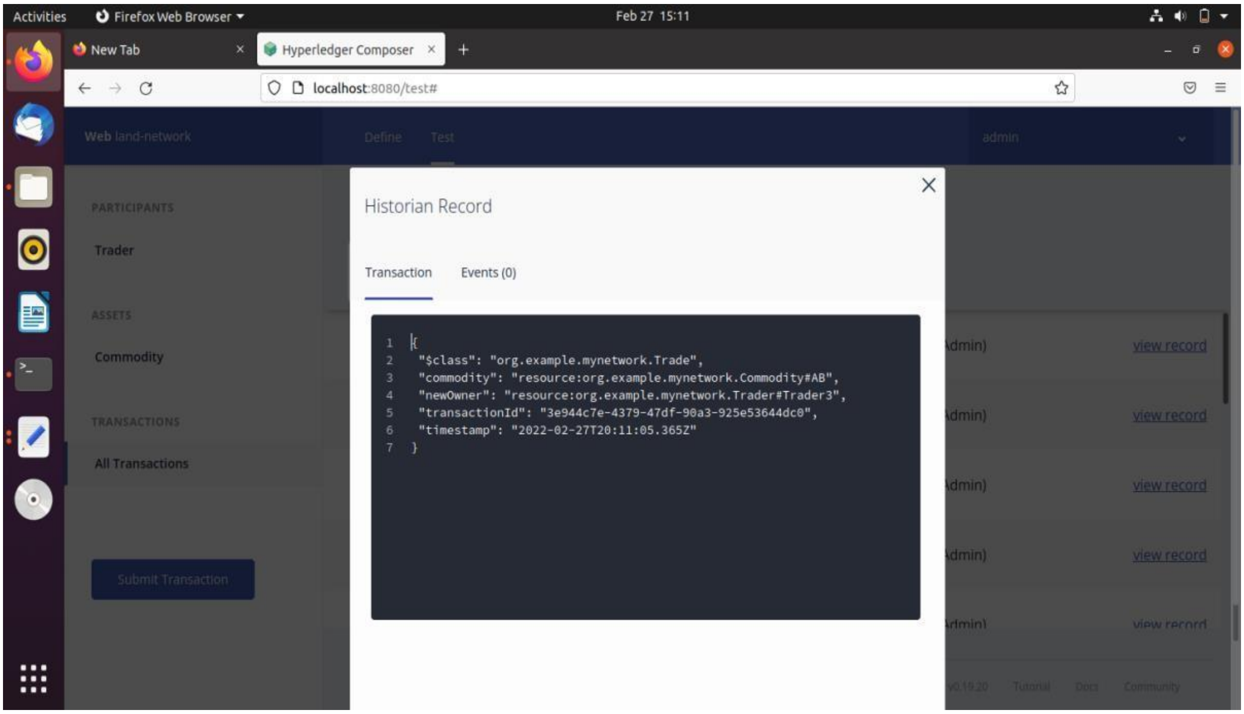


Figure 19. Transaction record with transaction ID and timestamp

6.4 Network Configuration

The network involves peers, orderers, assets, couch-db, chaincodes, and transactions. There three participants in this network: user, registrar authority, and authentication authority. The user and land register chaincode will be installed on registrar authority and the authentication chaincode will be installed on authentication authority which will be added to the channel with peers. Figure 20 shows the essential docker images of the network.

Figure 20. Essential actors of network

 ISSN: 3079-5354

6.5 SDK Layer

For the application implementation we will use the Fabric SDK which offers Fabric Gateway API and Client Gateway API depending on the Hyperledger Fabric version to generate and implement the user application with node.js language using with REST server to provide the service to interact between the client API and the network. The application will focus on three tasks:
- *Tokenization of the land***:** Tokenization on Hyperledger fabric is implemented by Erc-20 standard to issue non-fungible tokens or customized tokenization. *Authentication:* Using Google OAuth 2.0 with REST server to allow the Google OAuth scheme to access to the network and interact with user and network. Figure 21 [35] of Hyperledger documentation shows the flow of Google OAuth 2.0 process with REST server, client, and the network.

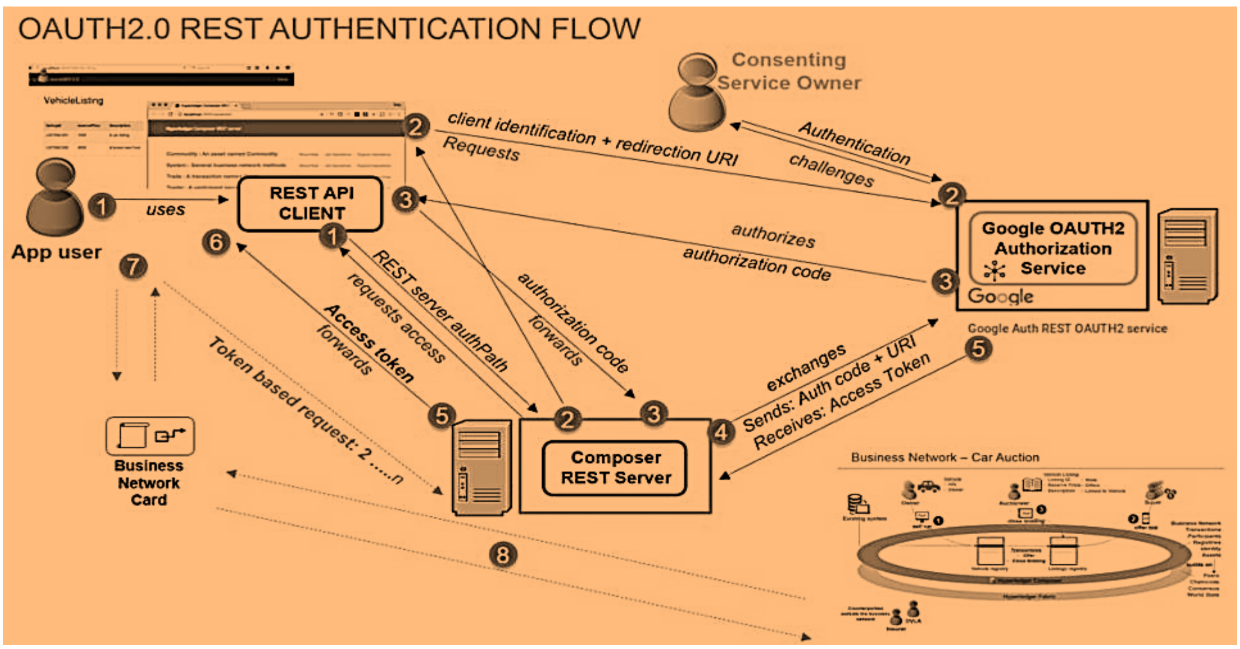


Figure 21. Google OAuth 2.0 scheme flow

- *Hashing***:** blockchain has the property of hashing that is utilizing SHA-256 hashing algorithm. As there were an added task to the research earlier to store the hash of the user sensitive information in the blockchain instead of the information in plaintext, it will bedeveloped utilizing the private data collection provided by Hyperledger Fabric as shown in figure 22 [36]. The private data collection involves two elements: the actual private data and the hash of that data.

- *The actual data:* Sent to the authentication authority as peer-to-peer communication and only stored on the database of that authority.

- *The Hash:* Will be stored on the ledger and it is endorsed, ordered, and stored in it. And is used for validation and audit. Also, it offers two types if implementation: Channel: this type is used when all the information in the ledger must be kept confidential. Collection: Is used when transactions or ledgers are shared among multiple organizations.

 ISSN: 3079-5354

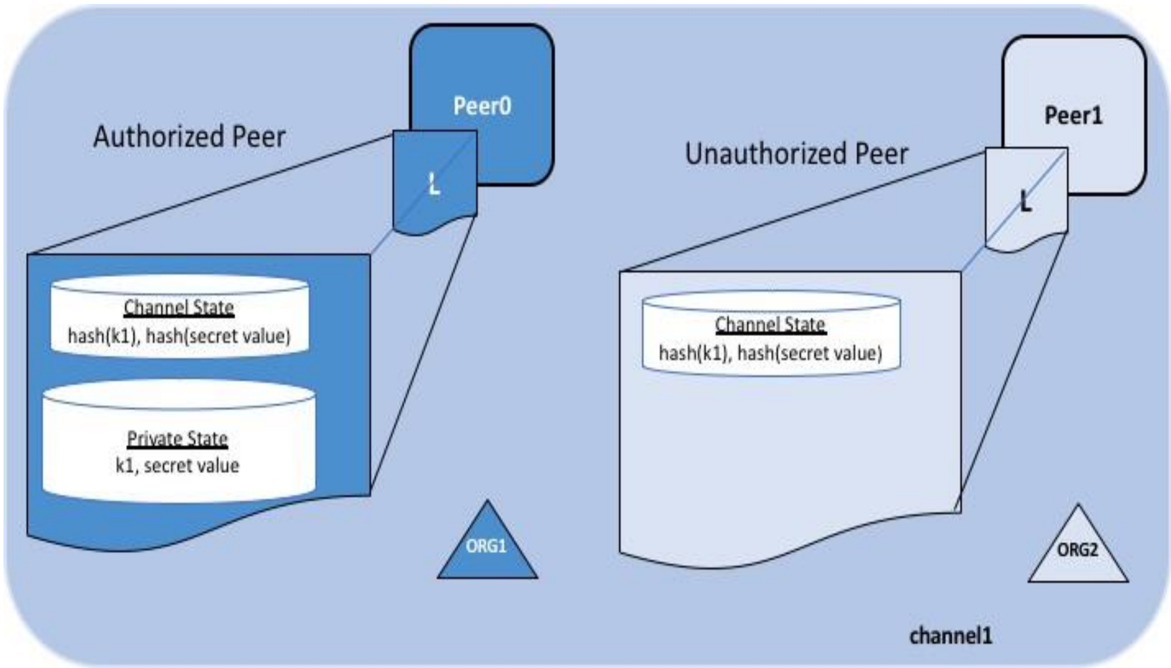


Figure 22. Concept of private data collection

***6.6** Use Case Testing:*

At the end of the implementation, the framework will be tested to validate its performance for:

- Users and land registration and information authentication by creating multiple clients and transactions.
- The tokenization of the assets.Effectiveness of private data collection for hashing and maintain confidentiality.

7. Analysis

7.1 Performance

Hyperledger fabric is widely used for private blockchain applications, such applications have high performance requirements and measured by some metrics such as transactions throughput, latency, and block time. In our case, theses metrics are important and impact the effectiveness of the overall framework. Hyperledger fabric have long-term supported versions v1.x and v2.x and both are running Raft ordering service which is based on crash fault tolerance algorithm (CFT) and allows to setup and manage the network easily and handles crash fault nodes. Raft protocol shows that the transaction throughput and latency are highly impacted by the endorsement policy (OR/AND), it has and increased throughput and lower latency with OR endorsement policy and lower throughput and increased latency with AND endorsement policy which affect the overall performance of the system and make it slower. Also, Raft ordering service is based on leader-follower nosed which means that. Only one node (the leader) is handling all the transactions and proceed them to all followers which increase the load on only one node that may crash if the performance reaches the peek. This provides the possibility that node may crash and there will be awaiting time until the new leader be elected.

Due to the impact of endorsement policy on Raft ordering service and transactions and the fact that Hyperledger fabric is based on CFT consensus algorithms, this can be considered as a limitation of fabric. Since Hyperledger fabric provides pluggable consensus to be adopted some researchers proposed ordering service based on BFT variations which provides the same level of safety and enhance the performance of transaction. The general idea of these proposed ordering service is to handle the transactions on multiple leader nodes and the ability to operate the transactions smoothly when a leader node crashed.

7.1 BFT variations for Hyperledger Fabric

Authors [37] proposed a BFT-based ordering service that is implemented on BFT-SMaRt to overcome the limitation of the platform and to enhance the throughput of transactions. The proposed ordering service allows to achieve up to 10,000 transaction per second and writing transactions to the blockchain in half a second. The architecture of the proposed ordering service is shown in figure 23, it consists of two parts: frontend and ordering cluster.

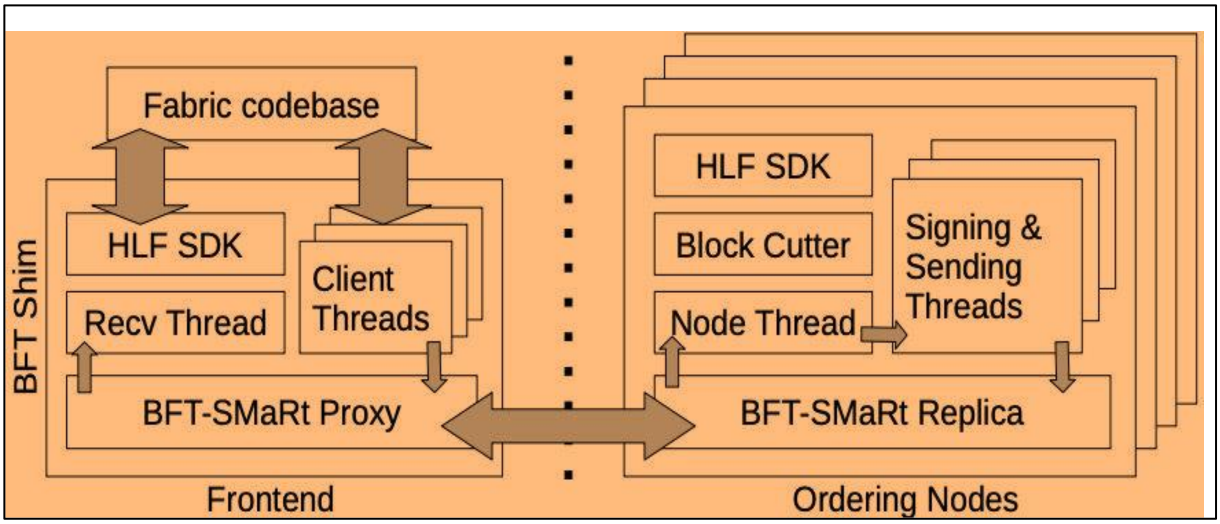


Figure 23. BFT-SMaRt Ordering Service

The ordering cluster consists of a set of nodes that collect the transaction from the frontends and executes the ordering service on the received envelopes. Then creates a block contains these envelopes attached with hash of the previous block in addition to a digital signature for the created block. Frontends receives transactions from clients through the Fabric codebase and relay them to the ordering cluster through BFT-SMaRt proxy. The flow of the ordering service as following:

1. Clients submit transaction through fabric codebase (client interface), Client Threads will receive the transactions and relays them to BFT-SMaRt proxy.
2. BFT-SMaRt proxy relays the transaction to the ordering cluster and receives the ordered blocks.
3. BFT-SMaRt Replica receives the transactions in ordered manner and relays them to Node Thread.
4. Node Thread will submit transactions from Blockcutter and assembles the next block.
5. Signing and Sending Thread signs the block and submit them to BFT-SMaRt Replica which can be submitted to the proxy to the Received Thread.

The proposed ordering service allows high number of transactions to be processed in suitable time and provides capability of durability in case if all or most ordering nodes fail and reconfigure a new ordering cluster by using the header of the last block which contains all the required information to proceed with. Also, it provides the ability of validating transaction through signing and sending thread before signing the blocks digitally and if the validation fails the transaction will be removed of the block, this allows to avoid performing transaction's validation by the ordering service after creating the block. This ordering service will not work efficiently on fabric due to the nature of the fabric infrastructure where it needs to be improved to fit the infrastructure, for example this ordering service provides the ability to withstand malicious ordering nodes by assembling blocks and signed them locally which results in a stream of blocks appended to the local copy of ledger, but fabric only allows stream of envelopes. This ordering service provides acceptable level of security, safety, and performance if the fabric infrastructure improved to support BFT algorithms without pluggable extensions. Authors [38] proposed a PeerBFT algorithm that extend the ordering service of the Hyperledger fabric by including peers auditing operation to the ordering service. The extended ordering service is shown in figure 24, the auditing operation will add two components to the ordering service: Auditor (to monitor the behavior of ordering nodes) and Changer (configure new order service nodes after confirmation of malicious behavior).

- Auditor

Auditor consists of two components Generator and Analyzer, after receiving a block each peer issues an audit transaction for each received block. For the analyzer, they defined an agreement level for the local ledger on peers. There are three levels: none, prepared, and committed which the level is updated depending on how many peers observed the block in their local ledger. The block will start with none level which indicated the block is new and appended to a peer's local ledger, which means the block is only chained on this peer local ledger. Then, the block level is updated to prepared when peers more than or equal to $n - f$ (n is the total number of peers, f is the maximum number of malicious peers) observed that block on their local ledger. Finally, the agreement level of block is updated to be committed when peers more than or equal to $n - f$ observed the prepared block on their local ledgers.

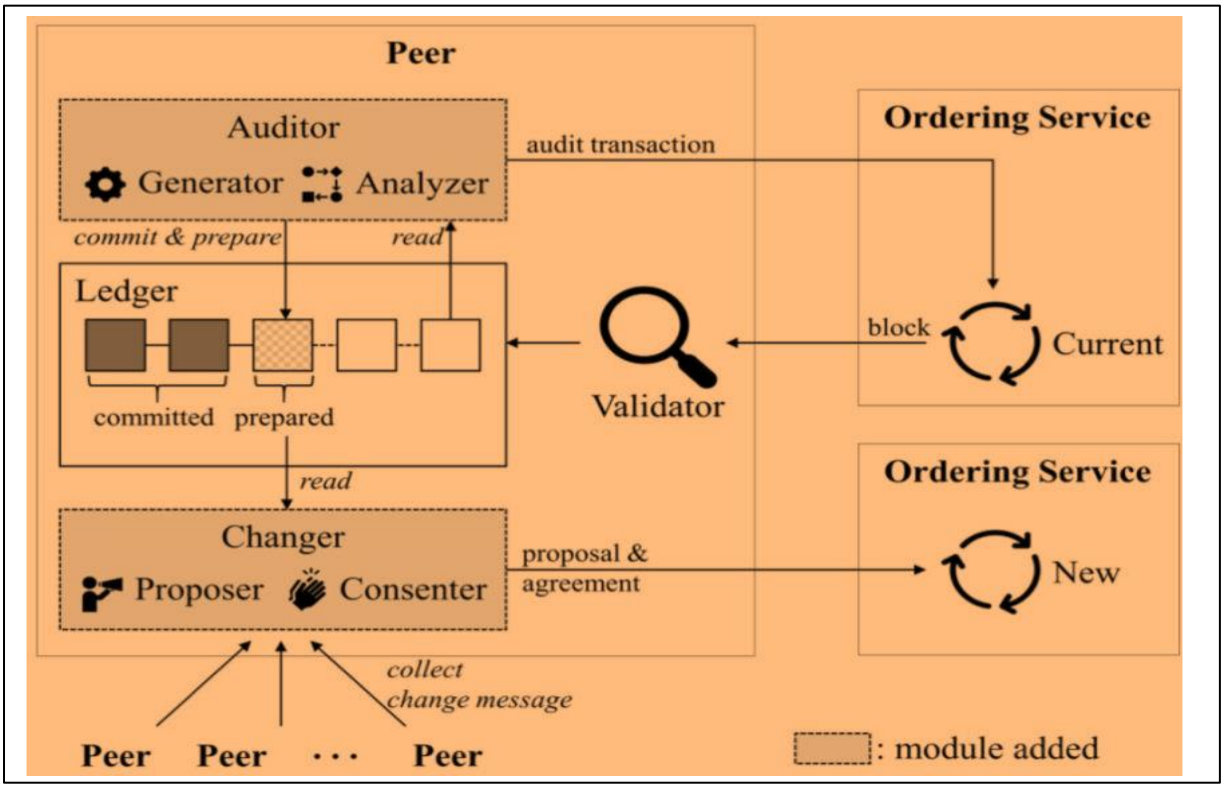


Figure 24. PeerBFT Extended Ordering Service

- *Changer*

This operation is designed to correct the ordering service after detecting malicious peers as following:

1. Broadcast change message: if a peer detects a malicious behavior of ordering service, peer will stop receiving blocks and it will be rejected and broadcast a change message.
2. Propose a new view proposal: when a peer receiving view change messages more than or equal $n - f$, it will issue a new proposal.
3. Agreement on new view: a peer should listen to the new proposed ordering service and expect blocks from the new view to complete the change operations.

This ordering service focuses on correcting the ordering service to delivered valid transactions in case of malicious behavior without affecting the flow of the system and loosing transactions. This protocol can be adopted on Hyperledger fabric with BFT-SMaRt since the PeerBFT is running on peers not ordering service. Authors [39] proposed Mir-BFT as a robust Byzantine fault tolerance protocol that allows multiple leaders in the ordering service to process independently and in parallel. This proposed protocol provides a robustness against malicious ordering service behavior that dropping or delaying client's requests and mitigate the probability of request duplication by a client. Mir partitions the request hash space into buckets of equal size and assign each bucket to a leader which it is only allows to process requests from the assigned buckets. The proposed protocol provides security and robustness against duplication attacks with its novel properties.

8. Conclusion and Future Works

The main purpose of this research is to provide systematic review to analyze proposed blockchain-based framework for land administration, highlight the main issues with land administration systems, and to find whether is there possibility to provide fully automated blockchain-based land administration within the current state of the blockchain technology in such a system. Also, to answer the research questions which resulted in there is a possibility to provide robust system against double spending by providing fully automated blockchain-based system or utilizing tokenization mechanism and mitigate tampering by managing users' identity to trace transactions and using consensus protocols. In section 2, we provide a background of blockchain technology and adoption of this technology to existed systems and highlight some of the important vulnerabilities in the blockchain technology. We proposed a private blockchain framework to be developed on Hyperledger Fabric and the important characteristics of the selected platform that will help to solve the main security concerns of this research. As a result of our research and the best of our knowledge is that there are no highly secure mitigation for malicious attacks such as the double request/spending, therefore we find that there is a need to improve the current consensus algorithms with concerns of these attacks. We will propose a consensus algorithm to enhance the current security level as mentioned. In section 7 and test it with the same framework. Our proposed framework is implemented on Raft protocol, and it provides the ability to process transactions, represent lands in blockchain and using non-fungible tokens. There is further work that is needed to enhance the security of our framework by designing and implemented a consensus protocol to be adopted in our framework, such as adopting the PeerBFT with some improvements to enhance the security and reduces the probability of malicious nodes by running it on the ordering service and integrating the Mir property to mitigate the duplication attacks. Another concept is newly proposed specifically to improve the security of land registry blockchain-based systems which is Bitsquares. The concept is representing from Bitcoins to Bitsquares, by replacing the coins with land's squares as the units of the transaction, with each square has a unique ID and the right holders on the blockchain. This concept allows to mitigate the double spending where each square has an ID with holder information so it can be traceable in addition with the Mir property the will provide a robust security and also provide the reliability of records that is stored in the land administration management system.

Corresponding author

Muhammad Mehboob Yasin
mmyasin@kfu.edu.sa

Acknowledgements
Not applicable.

Funding
This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University.

Contributions
S.A; M.M.Y; Conceptualization, S.A; M.M.Y; Investigation, S.A; M.M.Y; Writing (Original Draft), S.A; M.M.Y; Writing (Review and Editing) Supervision, S.A; M.M.Y; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests.

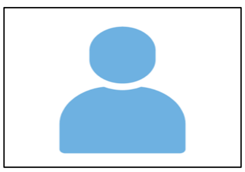
References

[1] Landerreche, E., & Stevens, M. (2018). *On immutability of blockchains*. In W. Prinz & P. Hoschka (Eds.).
[2] National Institute of Standards and Technology. (2018). *Blockchain technology overview* (NISTIR 8202).
[3] Lemmen, C., Vos, J., & Beentjes, B. (2017). Ongoing development of land administration standards. *EPLJ*.
[4] Williams, I. (2020). *Cross-industry use of blockchain technology and opportunities for the future* (1st ed.). IGI Global.
[5] Kaczorowska, M. (2019). Blockchain-based land registration: Possibilities and challenges. In *Proceedings of the 16th International Conference Cyberspace*.
[6] Bennett, R., Miller, T., Pickering, M., & Kara, A. K. (2021). Hybrid approaches for smart contracts in land administration: Lessons from three blockchain proofs-of-concept. *Land*.
[7] Schdev, D., Chakrabarti, D., & Mittal, A. (2019). Review of ownership-based blockchain frameworks in government applications. *IITM Journal of Business Studies (JBS)*.
[8] Davies, E., Kirby, N., Bond, J., Grogan, T., Moore, A., Roche, N., Rose, A., Tasca, P., & Vadgama, N. (2020). *Towards a distributed ledger of residential title deeds in the UK*. Mishcon de Reya.
[9] Alkhalifah, A., Ng, A., Kayes, A. S. M., Chowdhury, J., Alazab, M., & Watters, P. (2019). A taxonomy of blockchain threats and vulnerabilities. *Preprints*.
[10] Thakur, M. (2017). *Authentication, authorization and accounting with Ethereum blockchain* [Master's thesis]. University of Helsinki.
[11] Konashevych, O. (2020). General concept of real estate tokenization on blockchain. *EPLJ*.
[12] Konashevych, O. (2020). *Tokenization of real estate on blockchain* [Doctoral dissertation]. Tilburg University.
[13] Muller, H., & Seifert, M. (2019). Blockchain, a feasible technology for land administration? In *Geospatial information for a smarter life and environmental resilience*.
[14] Marsalek, A., & Zefferer, T. (2019). A correctable public blockchain. *IEEE*.
[15] Ahmad, D., Lutfiani, N., Ahmad, A. R., Rahardja, U., & Aini, Q. (2021). Blockchain technology immutability framework design in e-government. *Public Administration Journal*.
[16] Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE*.
[17] Shuaib, M., Mohd Daud, S., Alam, S., & Zada Khan, W. (2020). Blockchain-based framework for secure and reliable land registry system. *TELKOMNIKA Telecommunication, Computing, Electronics and Control*.
[18] Bahalul Haque, A., & Rahman, M. (2020). Blockchain technology: Methodology, application and security issues. *International Journal of Computer Science and Network Security*.
[19] Bhanupriya, P., Gauni, S., Kalimuthu, K., & Manimegalai, C. T. (2021). A modified hybrid blockchain framework for secured data transaction. *Journal of Physics: Conference Series, ICACSE 2020*.
[20] Singh Yadav, A., & Singh Kushwaha, D. (2021). Digitization of land record through blockchain-based consensus algorithm. *IETE Technical Review*.
[21] Krishnapriya, S., & Sarath, G. (2020). Securing land registration using blockchain. *Elsevier*.
[22] Iqbal, M., & Matulevičius, R. (2021). Exploring sybil and double-spending risks in blockchain systems. *IEEE*.
[23] Soner, S., Litoriya, R., & Pandey, P. (2021). Exploring blockchain and smart contract technology for reliable and secure land registration and record management. *Springer*.
[24] Pereira, S. N., Tasnim, N., Sunny Rizon, R., & Islam, M. N. (2021). Blockchain-based digital record-keeping in land administration system. *ResearchGate*.
[25] Gupta, N., Lal Das, M., & Nandi, S. (2019). LandLedger: Blockchain-powered land property administration system. *IEEE*.
[26] Singh Yadav, A., Agrawal, S., & Singh Kushwaha, D. (2021). Distributed ledger technology-based land transaction system with trusted nodes consensus mechanism. *Elsevier*.
[27] Devi, D., Sai Rohith, G., Shri Hari, S., & Sri Ramachandar, K. (2021). Blockchain-based mechanism to eliminate frauds and tampering of land records. *ITM Web of Conferences*.
[28] Begum, A., Tareq, A. H., Sultana, M., Sohel, M. K., Rahman, T., & Sarwar, A. H. (2020). Blockchain attacks, analysis and a model to solve double spending attack. *International Journal of Machine Learning and Computing*.
[29] Lee, H., Shin, M., Kim, K. S., Kang, Y., & Kim, J. (2018). Recipient-oriented transaction for preventing double spending attacks in private blockchain. *IEEE*.
[30] Nandi, M., Bhattacharjee, R. K., Jha, A., & Barbhuiya, F. A. (2020). A secured land registration framework on blockchain. *IEEE*.
[31] Nicolas, K., & Wang, Y. (2019). A novel double spending attack countermeasure in blockchain. *IEEE*.
[32] Balaji, S. (2017). Blockchain based secure smart property registration management system and smart property cards. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*.

ISSN: 3079-5354

[33] Hyperledger. (n.d.). Retrieved from http://www.hyperledger.org.
[34] Androulski, E., Cachin, C., Ferris, C., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., & Stathakopoulou, C. (2019). Hyperledger fabric: A distributed operating system for permissioned blockchains. *IEEE*.
[35] Google OAuth 2.0 Scheme. (n.d.). Retrieved from https://hyperledger.github.io/composer/v0.19/tutorials/google_oauth2_rest
[36] Private Data Collection on Hyperledger Fabric. (n.d.). Retrieved from https://hyperledger-fabric.readthedocs.io/en/release-2.2/private-data/private-data.html
[37] Sousa, J., Bessani, A., & Vukolić, M. (2018). A Byzantine fault-tolerant ordering service for the Hyperledger Fabric blockchain platform. In *Proceedings of the 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*.
[38] Jeonghyeo, M., Yongrae, J., & Chanik, P. (2020). PeerBFT: Making Hyperledger Fabric's ordering service withstand Byzantine faults. *Institute of Information and Communications Technology Planning and Evaluation (IITP)*.
[39] Stathakopoulou, C., David, T., Pavlovic, M., & Vukolic, M. (2021). Mir-BFT: High-throughput robust BFT for decentralized networks. *IBM*.

Biographies



Sarah Alyounis received a master degree in Cybersecurity from King Faisal University. He has an excellent experience in the cybersecurity field in both theoretical and practical. He has several certificates in cybersecurity like CEH and others. He several publications in cyber risk assessment. His research interests including cyber security, risk assessment and cyber-attacks.

Prof. Muhammad Mehboob Yasin received the B.Sc. degree from the University of the Punjab, Lahore, Pakistan, in 1975, the M.Sc. degree in computer science from the University of Wales, Aberystwyth, U.K., in 1983, and the Ph.D. degree from The Open University, Milton Keynes, U.K., in 1986. He served in various research and development roles in Pakistan Atomic Energy Commission for over two decades, and then moved to academia, serving as a Professor, the Department Chair, and the Dean at renowned institutions in Pakistan. In 2009, he joined the prestigious Computer Laboratory, Cambridge University, U.K., as a Visiting Professor. He has been a (Full) Professor of Computer Networks with the College of Computer Sciences & Information Technology, King Faisal University, Saudi Arabia, since 2011. His research interests include computer networks, applied cryptography, the Internet of Things, and cybersecurity. mmyasin@kfu.edu.sa