PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
MINISTRY OF HIGHER EDUCATION AND
SCIENTIFIC RESEARCH

IBN KHALDOUN UNIVERSITY - TIARET

A THESIS

Presented to:

FACULTY OF MATHEMATICS AND INFORMATICS
COMPUTER SCIENCE DEPARTMENT

Submitted in partial fulfillment of the
requirements for the degree of:

Master in Software Engineering

By:

SARMOUM Ahmed

Réalisation d'un livre foncier securisé par la Blockchain

(Realization of a land book secured by the Blockchain)

Publicly defended in Tiaret by the committee composed of:

Mr. CHADLI Abdelhafidh	M.C.A	IBN-KHALDOUN university -Tiaret	President
Mr. MERATI Medjeded	M.C.A	IBN-KHALDOUN university -Tiaret	Reviewer
Mr. KHARROUBI Sahraoui	M.C.A	IBN-KHALDOUN university -Tiaret	Supervisor

2021 -2022

ACKNOWLEDGMENTS

First and foremost, thank ALLAH who gave me strength and the Patience to accomplish this modest work.

A very big thank to:

My parents who followed us during our studies

I would like to thank my supervisor **Mr. KHARROUBI Sahraoui** *for his confidence, and* **Mr.TASSALIT Ahmed** *for his feedback and adjustment of the research.I would also like to thank the committee consisting of* **Mr. CHADLI Abdelhafidh and Mr. MERATI Medjeded.**

As we don't forget **Mr.SARMOUM Mohamed**, *a worker at Theniet El Had real estate sector, for his support and assistance.*

Secondly, we would like to thank all teachers and staff at UIK for help and support during our studies.

DEDICATION

To my parents

The reason of what

I become today.

Thanks for your great sup-

port and contious care .

To my friends

Thank you for be-

ing in my life.

Abstract

Land registries succeed when trust is assured between all parties involved. In this study we try to improve the quality of land records using Blockchain technology. By using the Blockchain, we can overcome the limitations (such as centralization) of existing land registries and provide a reliable service that delivers significant benefits. Blockchain technology and distributed ledgers provide trusted, immutable and distributed records of transactions and support decentralization, and Blockchain adoption may be more beneficial for records with a perpetual retention schedule. This is because the hash value, which is a feature of the Blockchain, stands as metadata for validating transactions. Moreover, the Blockchain registry does not require a central party, and Blockchain record keeping solutions may also enable better protection for citizens and governments.

Keywords: ledger, registry.

الملخص

تنجح سجلات الأراضي عندما يتم ضمان الثقة بين جميع الأطراف المعنية. نحاول في هذه الأطروحة تحسين جودة سجلات الأراضي باستخدام تقنية البلوكشين. باستخدام البلوكشين ، يمكننا التغلب على القيود (مثل المركزية) لسجلات الأراضي الحالية وتقديم خدمة موثوقة تقدم فوائد كبيرة. توفر تقنية البلوكشين ودفاتر الأستاذ الموزعة سجلات موثوقة وغير قابلة للتغيير وموزعة للمعاملات وتدعم اللامركزية ، وقد يكون اعتماد البلوكشين أكثر فائدة للسجلات ذات الجدول الزمني للاحتفاظ الدائم. هذا لأن قيمة التجزئة ، وهي إحدى ميزات البلوكشين ، تقف بمثابة بيانات وصفية للتحقق من صحة المعاملات. علاوة على ذلك ، لا يتطلب سجل البلوكشين طرفًا مركزيًا ، وقد تتيح حلول حفظ سجلات البلوكشين أيضًا حماية أفضل للمواطنين والحكومات.

الكلمات المفتاحية: الدفتر الموزع، السجلات.

Contents

List of Figures

Chapter 1

Land Registry (The Cadastre)

1.1 Introduction

The word cadastre does not have a clear etymology. For some authors, it may come from the term "CATASTICO" from the Greek "KATASTIKHON" which means to list; Or even the word "Latin" came close to "capitestra", a term in ancient Rome referring to records containing the list of goods and their owner's statement. [2]

Cadastre is a collection of documents compiled systematically from topographical and land surveys. In other words, it is an inventory of land ownership that provides a fairly detailed description, and it is intended to meet individual or collective needs, especially related to land and financial matters. [1]
Through this inventory, we are able to:

- The cadastral chart (graphic document)
- Land records (literal documents)

For this reason, some authors consider the land registry to be the civil status of land ownership

1.2 Purpose of the land registry

Generally, a land registry consists of a blueprint, a plot record, a landlord's record, and some additional records. The current globalization of the real estate field through the management of data in databases or geographic information systems and the use of information technologies such as the proposed Blockchain technology will provide many benefits to this important sector.

- Advantages of the land registry

1. It is necessary to establish a well-functioning registration system in order to make sure that the legal status of the land is clear, as well as that of the parties involved and third parties. In this way, the investor or owner is provided with more security.

2. Facilitating the loan-granting process by financial institutions. In addition to reducing disputes, legal certainty reduces the number of different borders, saving both time and money and building good neighborly relationships.

3. Due to the fact that land is a source of income, and that the land registry is needed to collect this income legally, taxation has become simpler.

4. In addition, there are other opportunities for obtaining information, the Land Registry already provides the necessary data for implementing national works, such as land compilation, planning, statistics, and town planning.

1.3 Land registration in Algeria

The National Cadastre Agency is a public administrative establishment, under the supervision of the Ministry of Finance. It is responsible, within the framework of the policy drawn up by the government, for carrying out the technical operations that should lead to the establishment of the general cadastre over the

whole of the national territory.[1]

In the Cadastral Registry, real estate plots are listed, their owners identified, and property boundaries determined. The end result is a set of documents that will help identify the ownership of the property:

- Graphic, THE CADASTRAL MAP
- Literally, LAND REGISTERS (CADASTRAL MATRIX)
- Graphical databases
- Literal databases in SGBDR Ingres[2]

Ordinance No. 75-74[3] amended and supplemented by Decree No. 92-134[4] confer on the cadastre the legal character, in effect:

- The cadastre serves as a source of information about the physical condition of buildings and is the basis for the real estate file (land book).
- The land book establishes the legal situation of the buildings, held in the form of a real estate file, proving the published rights.

Assignees of land matters are classified as cadastre and conservation areas, with the cadastre responsible for identifying buildings and giving their physical description, while areas conservation specify their legal status.

The land mission of the cadastre therefore consists mainly of two series of operations:

- **the identification of buildings:** Cadastral references are required to identify any act subject to land registration formalities. Property blocks are land units consisting of plots owned by the same owner and located in the same location.
- **their physical description:** Surface, Limits are two operations that make it possible to describe the physical characteristics of a building

[1] (cf. Decree 89-234 creating the N.C.A. modified and completed).
[2] (INtelligent Graphic RElational System)
[3] No. 75-74 of November 12, 1975, and Decree No. 76-62 of March 25, 1976.
[4] No. 92-134 of April 7, 1992

a- the determination of the limits (DELIMITATION): To identify the limits on the ground of a property, its delimitation is necessary in order to determine its material consistency. There are several formalities associated with it, including:

- summons of persons (owners)
- verification of the identity of the owners
- recognition of each building
- report of limits

The limits shown on the cadastral plan are generally the representation of the property, but they will become definitive once the publication formalities are completed.

b- surface calculation: The determination of the cadastral content of the blocks is carried out using the planimeter or numerically using the coordinates.

1.4 Problem Statement

In our project, we are trying to develop a land registry in Algeria using Blockchain technology. In light of the traditional method, which is slow, cumbersome, and prone to fraud and corruption, this project offers a meaningful and commercially viable solution to an issue that we call "proof of concept" in the land registry area. Having said that, what is the problem with land registries anyway, and why does Blockchain seem to be the answer?

> *'Historical geography can be understood today as the restitution at a given moment of a geographical state which, moreover, may have escaped the men of that time. It is the reconstitution of the geographical past.'* (Ch. Higounet)

Land is a series of social relationships that are supported by territorial space. Public policies and spatial planning determine these relationships specifically when considering historical, economic, legal, and spatial factors

Land development and its implications for economic and social development pose a challenge to the whole society, and particularly the public authorities re-

garding the mechanisms to be put in place and the measures to be implemented to achieve a coherent, harmonious and balanced approach in different places. As part of sustainable development, this choice is essential

It is the unprotected citizens who suffer the most from the current land registry system, which is rife with corruption and inefficiency. Hundreds of cities in developing countries suffer from similar problems with land records. Many citizens simply do not trust the system. Some are not sure if they legally own a plot of land, even if they have a legitimate deed of sale. Others who want to buy a plot of land are not sure if the seller legally owns it.
Today, the land situation in Algeria remains complex and problematic:

- Having a policy without a clear definition makes things complicated. The conditions for supply and demand generate "irrational" prices as a result of speculation that disturb the buyer.

- Due to the fact that the forces that dominate the market typically engage in strategies and/or practices that contribute to a damaging situation, access to the ground is difficult and delicate.

1.5 Examples of Blockchain use cases

The application of this technology is being pursued by a number of government and non-governmental organizations around the world. It is already being implemented by some. Immutable trustworthy records can be created using this technology without the need for trusted third parties.

An example of this is the sale of land. Traditionally, land transfers involve listing the property on a real estate market, negotiating the price, and registering the sale with the state's land titles registration authority after the sales contract has been exchanged.The traditional method of transferring land is slow and cumbersome, often involves manual recording of transactions by land authorities, and can be vulnerable to fraud and corruption.

The Georgian government, for example, has been using Blockchain technology to register land titles from 2016 and is planning to extend the service to sales,

purchases, mortgages, rentals, new land title registration, property demolition and notary services as well [18].

Sweden's land registration authority, Lantmäteriet, is integrating a Blockchain into its recording of property transactions and is expected to save $106 million annually by reducing paperwork, eliminating fraud, and speeding up the process [4].

In Pelotas, Brazil, the local real estate registration authority recently launched a pilot project using blockchain technology for land transfer registration [3].

1.6 Conclusion

A discussion was conducted in this chapter about the Land Registry and some of its various missions. We also talked about some points of the complex and confusing situation of the current approved land registry system in Algeria.In the next chapter we will talk about the second key element on which our graduation project is based on , which is Blockchain technology.

Chapter 2

Blockchain technology

2.1 Introduction

Blockchain and distributed database technology have burst onto the scene in the past few years as an important future technology. Internationally agrees upon the definition of Blockchain or distributed database [19], they are described as "an open-source technology that supports trusted, immutable record of transactions stored in publicly accessible, decentralized, distributed databases". According to most technology research and advisory firms, over the past few years, these technologies have become the most popular innovations. Governments and organizations around the world are beginning to look seriously at the application of this technology and some have already implemented it.

2.2 Historically

According to ***Marley Gray***[1],2008, a person or group of people known as ***Satoshi Nakamoto*** has published an article describing Bitcon and how it could be used for digitization. Send payments between tow consenting enters without the need for a third financial institution, Each transaction was recorded on the Blockchain register, the digital signature. To ensure confidence in the great book,

[1]**Marley Gray**, Diector of the Tecknology Strategy for Financial Services at Microsoft

network participants must perform complicated algorithms to verify these digital signatures before adding transactions to the Blockchain.

The next few years for bitcoin have been tumultuous, including the collapse of first-plan Bitcoin Exchange. **MT. Gox**[2], is a more and more reputation as the currency fueling the online drug bazaar. But many companies have seen an opportunity in the underlying technology – the Blockchain – with made possible the existence of bitcoin[7].

2.3 Definition

A blockchain is a distributed database of all completed digital events shared among participating nodes. All events that have happened are specifically and verifiably logged. A majority of the nodes in the Blockchain database validates each event unanimously. Public Blockchains and private Blockchains are the two major types of Blockchain. A public Blockchain is an open Blockchain where anyone can join and interact with it without obtaining permission from a central authority. Meanwhile, private Blockchains are protected by access control mechanisms. By regulating who is allowed to participate in the network and who can view, write to, and join the Blockchain, administrators can control who uses the network. Private Blockchains permit consensus groups to be created by administrators. In this way, private Blockchains can converge and become centralized, leaving them vulnerable to single points of failure. In contrast, public Blockchains are purely decentralized, have no single point of failure, and are resistant to malicious attacks. As soon as a node is connected to peers in a public blockchain, it first attempts to create a full Blockchain.[26]

By using cryptography, each block on the Blockchain is linked cryptographically to the block before it to ensure that nobody can alter the data contained within them without being noticed. As a result, it is deemed unnecessary to establish a trust relationship between users.

[2]**Mt. Gox** was a bitcoin exchange based in Shibuya, Tokyo, Japan.

2.4 Block Structure

A Blockchain is a chain of blocks each containing several transactions see *fig 2.1*, and which will be registered progressively in the Blockchain by nodes of the network. The implementation may differ from one Blockchain to another [7], but the main elements of a block are:

- **An index:** this is the block number.
- **A hash used to identify the block:** the value of the hash associated with the block.
- **The hash of the previous block:** the value of the hash associated with the previous block.
- **A timestamp:** the block creation time.
- **A set of transactions:** the set of transactions performed.

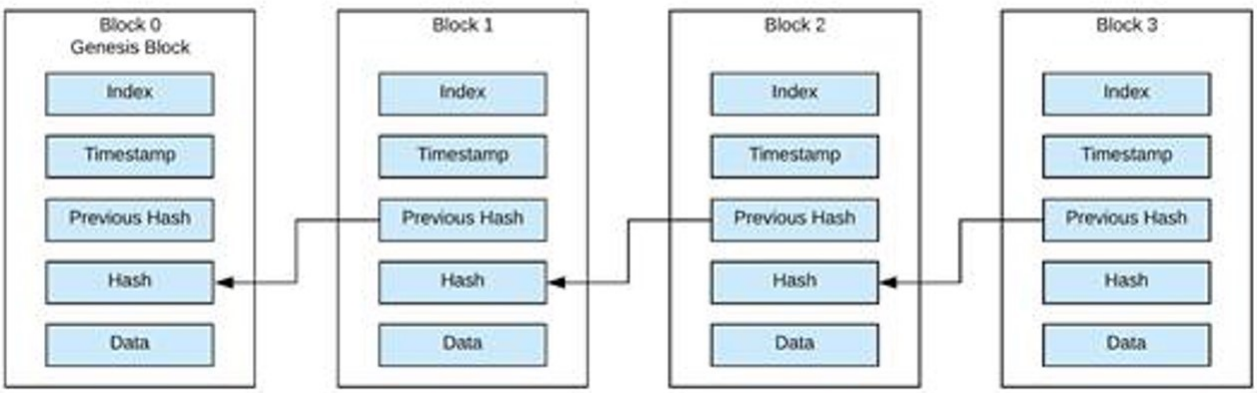

Figure 2.1: Block structure in Blockchain

2.4.1 Proof of work (Nonce)

Proofs of work (Nonce)[3] are random numbers created by pseudo-random number generators and have the property of being unique in a system. In order for the proof of work to be valid, the block header hash must be less than a certain number called the threshold, which is determined by the difficulty. As the first 4 pieces of information change with each block and it is impossible to predict the value of the hash without applying the SHA-256 function, the only way to obtain a valid hash is to test different proofs of work until obtaining a hash corresponding to the level of difficulty.

We understand here that the lower the threshold, the greater the number of 0s required at the start of the hash, and therefore the more difficult it is to find a valid proof of work.

As part of the Bitcoin Blockchain, transactions (addresses, amount, signature) are grouped into blocks every 10 minutes. For a block to be non-repudiable, a minor must have validated it and transmitted it through the network. The validation of a block is carried out as follows:

Lists of transactions are pending in the nodes.

Miners must calculate the cryptographic sum (a hash) of this list associated with other elements: timestamp, identifier of the previous block as well as a nonce of the block.

The hash value must start with a certain number of zeros determined by the network. Successive proofs of work are tried to arrive at this result. When a valid

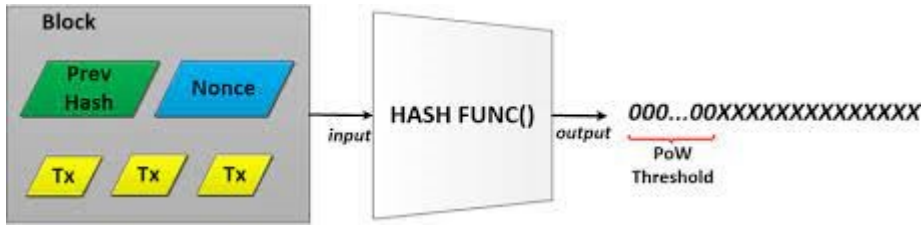

Figure 2.2: Proof-of-Work calculation

[3]Nonce is the central part of this Proof of Work

result is found (i.e. respecting the number of first bits at 0), it is transmitted to the other nodes which can easily verify the sum using the proof of work which was used to perform the operation. The more the number of zeros required increases, the lower the probability of generating a sum starting with them and therefore the more computing power will be needed to achieve this result. This number of zeros corresponds to the notion of proof of work. The more the size of the network increases, the more the computing power is important and the more it is necessary to increase the number of zeros in order to remain on a production of one block every 10 minutes [22].

2.4.2 Hash Value

The Blockchain is based on the principle of hash values. A hash value is a cryptography, ideally unambiguous value connected to a file, often referred to as its "fingerprint". The Blockchain docs not only generate specific hash values for electronic documents or other information (as compared to electronic signature processes) but also stores signed hash value serially in a kind of register (ledger function). A new hash value and the corresponding signature are added to the Blockchain file as a new block. In order to ensure the integrity (invariability) of the stored hash values, Blockchain application do not use central authority (like a trust service provider/certification authority), but rather rely on "swarm intelligence"[4] because the integrity of the ledger is protected by the multitude of its distributed copies on computers all over the internet "distributed ledger"[5].

For that reason, high availability is one of the advantages of a Blockchain system in its pure form. For the same reason, Blockchain neither "proves" the authenticity of a transaction (addition of a new hash value to the register) nor is the integrity of all hash values guaranteed by a central authority – for example as part of a public administration. Blockchains rely on "swarm intelligence"[4] insofar as information that is added to the chain will be acknowledged as valid if a majority

[4] **Swarm intelligence:** is the self-organization of systems for collective decentralized behavior. Swarm intelligence enables groups to converge and create an independent organism that can do things that individuals can't do on their own[24].

of the ledgers recognizes it as such[5].

In order to carry out a transaction, a signature is created with a private cryptography key that comprises the information of the transaction The signed transaction id then published to the network. Now all participants can verify it by extracting the public key of the signature of the sender and verifying the validity of the signature. If the signature corresponds to the transaction, the participants validate it. Thus, with Blockchain, tow parties who don't know each other should to able to agree that something is "true" without need for confirmation from an intermediary or a central authority.[5]

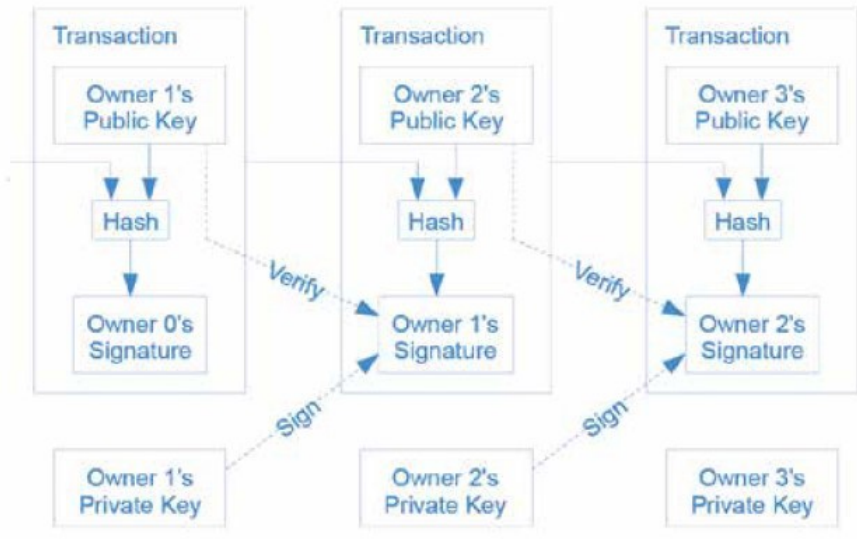

Figure 2.3: Blockchain structure. [23]

The Blockchain is based on an ideology that has an inbred skepticism towards public authorities. It tries to protect itself from interference by such authorities by subscribing to a distributed approach that cannot be easily controlled even by a central player. The flip side of this idea is that the trust needs to be placed in the system and its mathematical and computational tenets because there is nothing else that will serve as a trust anchor.

Due to its decentralization, the Blockchain has to be public – otherwise there would be no way to generate the necessary number of participants to achieve the necessary degree of distributed because only hash values are stored, it is not possible without further information to connect actual transaction to a Blockchain proof – no conclusion can be drawn from them regarding content data.

At its core, Blockchain systems are anonymous that mean transactions are

connected by certificates. Blockchain itself does not reveal the identity of participants, neither will it provide information on which natural or legal person is connected to the certificate in real life. The Blockchain does not forgot: the deletion or change of a value that has become part of the Blockchain is virtually impossible[5].

2.5 Block verification

As soon as a miner has found a valid block, it transmits it to the network. Each node that receives this block checks its validity using the following algorithm:

- Check that the previous block exists and is valid (equivalent to checking that the hash of the last block corresponds to the "hash of the previous block" element referenced in the header of the block being checked) [17].
- Check that the date of the block is greater than the date of the previous block and less than 2 hours later [8].
- Check that the proof of work is valid (i.e. the block header hash is below the threshold) [17].
- Check all transactions. If any of them return an error, stop and return FALSE [8].
- Update the set of unverified transactions and return TRUE, If the algorithm returns true, the block is considered valid and the node adds it to the Blockchain. If this node is a miner, it then starts looking for the next block: it collects a new set of transactions from the set of unverified transactions and starts the proof of work again for this set.

2.6 Main values of blockchains

Blockchains guarantee the integrity of data and users. First, it is virtually impossible to alter or tamper with blocks on a chain, providing a high level of data integrity or immutability. Second, metadata about transactions performed by a node or an end user is stored in the Blockchain and can be linked to the

user performing them, this means that users cannot cheat the network or attempt to perform an invalid transaction. Although complete anonymity is impossible, Blockchains do not contain any personal information and use private/public encryption to authenticate the users performing the transactions. Nodes and users do not need to provide names or personal information to become part of the network, and mining Blockchains to obtain personal information to sell to third parties for profit is impossible.

2.6.1 Distributed trust

Blockchain circumvents the need for a trustworthy central authority. Instead, trust is distributed across network elements. The same goes for governance mechanisms; in principle, different types of users and nodes have the same political weight.

2.6.2 Main actors

The main developers have write access to the source code. All nodes hold up-to-date copies of the Blockchain, validate the new blocks and then broadcast them to the network. Miners are dedicated to proof of work. End users use the network to transact through client software or wallet software. Service Nodes like Wallets[5], Storage, Exchanges and Cloud Services.

2.6.3 Peer to peer technology (P2P)

In a peer-to-peer network, all interconnected nodes are in principle equal. Since there is no central server, there is no central point of failure. If one node fails, all other nodes remain interconnected; the data and information circulating in the network are thus preserved.

[5] **wallet:** is a device, physical medium, program or a service which stores the public and/or private keys for cryptocurrency transactions

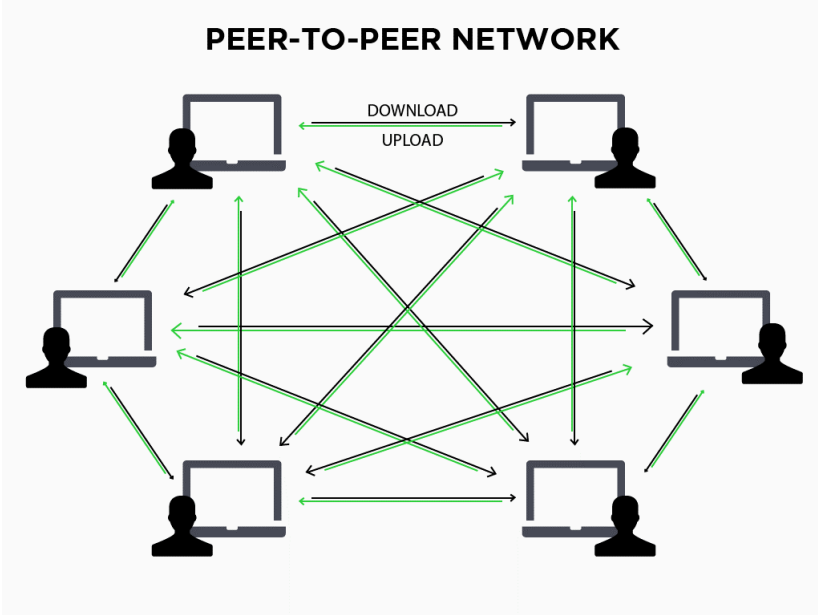

Figure 2.4: The peer-to-peer network (P2P)

2.6.4 Cryptography

The Blockchain uses public key cryptography, a private key that is known only to its owner, and a public key that is shared with the rest of the world. A private key is first randomly generated and then used to create a public key. The private key is used to encrypt the transaction which can then be decrypted by the intended recipient using the sender's public key. It is mathematically impossible to use a public key to decrypt a private key

2.7 Blockchain typology

There are three types of blockchain. Each corresponding to a specific scope:

2.7.1 Public Blockchain

It is a blockchain accessible to anyone in the world. No permission is required to carry out transactions or to participate in the consensus process. All actors are in an equal position in their participation in the network. Bitcoin and Ethereum are the two main public Blockchains.

2.7.2 Private Blockchain

It is a Blockchain running on a private network, in which all participants are known and for which governance is provided by an organization. No one can access and participate in it without permission.

2.7.3 Blockchain Consortium (Hybrid)

These are Blockchains in which the consensus process (validation of transactions/blocks) is controlled by a known and limited number of nodes. Some nodes can be made public (read-only access allowed) while others remain private. They are more suited to regulated contexts [10].

2.8 How a Blockchain works?

Transactions made between network users are grouped together in a data structure called a block. Blocks are ordered and prioritized in a single, unique chain. Each block points to the last valid previous block. This chain is "distributed" and "replicated" on all the nodes of the network. Each new transaction and/or Smart Contract, "pending", is grouped in a new block. For this block to be added to the Blockchain, it must be validated. This validation is carried out through certain specific nodes of the network called “miners”. The role of these nodes is to answer a complex crypto mathematical puzzle. Each response found is specific to one and only one block, thus prohibiting its reuse for the validation of a new block. The crypto/mathematical problem, specific to each block, is very difficult to solve. It requires significant computing resources and therefore financial resources (electricity, hardware maintenance cost, personnel cost, etc.). To encourage minors, who are essential to the proper functioning and viability of the network, remuneration is allocated to them as a reward for their work. The complexity of the validation problem is linked to a difficulty associated with the block.

In order to keep the production time of a block constant, the level of difficulty is automatically adjusted by the network. Extremely difficult to calculate,

the validation of the solution is, conversely, very easy. There are multiple valid solutions for a given block. It is enough to find at least one for the block to be validated through the consensus process. Once the block is validated by a "miner" and approved by the other nodes of the network, it is timestamped and added, at the top of the chain of blocks (last valid block created) and all the nodes of the network add it in their copies of the string. The figure below illustrates how a Blockchain works.

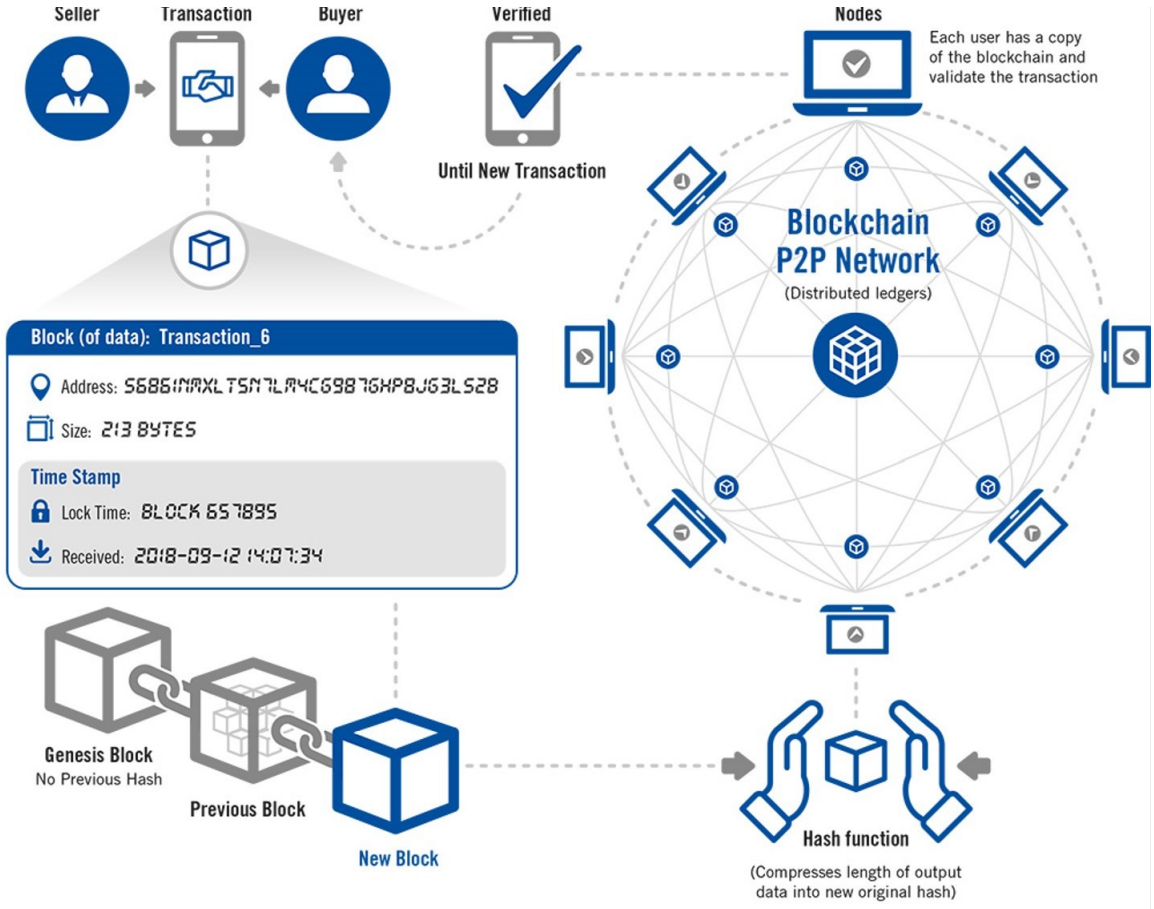

Figure 2.5: Blockchain and Distributed ledger Technology at Work

2.9 The case of the contradictory bloc

On a network, it is possible for two different blocks to be added at the same time by different nodes, creating a fork in the chain. In this case, there is a "consensus rule" that helps nodes determine which block to believe. In Bitcoin, the rule is called the "longest chain rule" - each node recognizes the legitimacy of the two competing blocks and the situation resolves when the next block is built on one of

the contenders. The longer chain becomes part of the Blockchain [11].

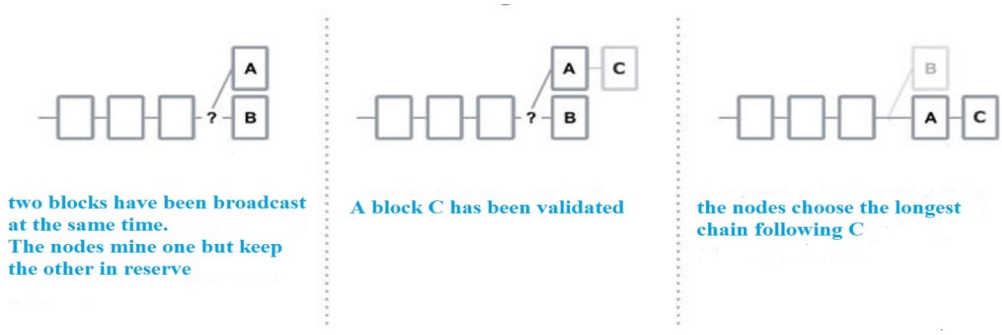

Figure 2.6: Resolution of the case of the contradictory bloc

2.10 What is transaction?

When individuals want to make a transaction on a Blockchain network, such as to transfer ownership of property, they transfer control of the asset by transferring the Blockchain representation of it (sometimes called a token) from their Blockchain address. An address is denoted by the hash of a public key – a hash that functions somewhat like a zip code by indicating the destination of a particular transfer of value. For each public key, there is a matched private key, the individual uses the private key to digitally sign the transaction to make the transfer of ownership happen.

The signature also prevents any modification of the transaction after it has been issued. Once signed, the transaction is "placed/deployed" on any node of the network which in turn broadcasts it, step by step, to all the nodes of the network. Now anyone on the network can use the issuer's public key to verify and ensure that the transaction request is coming from the rightful account owner. If the transaction is valid, it is then included, along with other "pending" transactions, in a block of the Blockchain, in turn "exploited" by miners

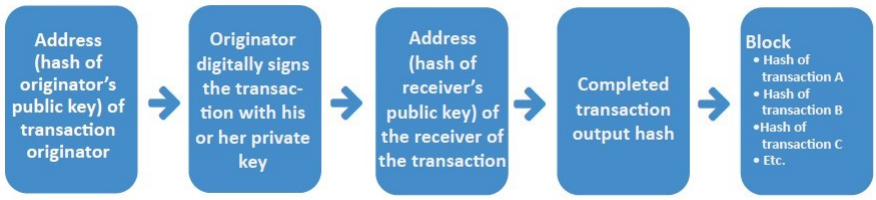

Figure 2.7: Transaction processing using public-private key pair on the Blockchain

2.10.1 The Hash of a transaction

A hash of a transaction is a double hash of the binary format of the transaction. The SHA-256 algorithm is applied twice, for historical reasons, and to increase security.

2.10.2 Transaction identifier

The hash code of a transaction is called the “txid” generally denoted “Tx”. This transaction ID is used to reference a transaction.

2.10.3 Cryptographic keys

A digital signature of a transaction is an encryption of the calculated transaction hash with a secret key. This secret key is called the private key. The signing of the transaction can be verified with an associated public key.

The digital signature proves that the transaction has not been modified and that this transaction was issued by the owner of the private key. The secp256k1 algorithm, based on elliptic curves (also called ’ECDSA’[6], is used for the digital signature of transactions.

This algorithm generates a new pair of encryption keys called private key and public key. The private key is a randomly generated 256-bit number. And the public key is calculated from this private key [7] (see fig 2.3).

2.11 New Block Creation (Mining)

Each newly created transaction gives rise to a "write" in a Blockchain. This write enters the network through a system node, which verifies and checks that its structure is correct with regard to the specifications of protocol implemented and that it is legitimate with respect to the writes already recorded.

[6] **ECDSA:Elliptic Curve Digital Signature Algorithm)**

If the write commit is satisfied, it is then "queued" in a local list and broadcast via the P2P (see fig 2.4) network to all nodes in the network. Otherwise, it is rejected.

Any user can be a network miner and all work simultaneously. They are free to choose which writings they incorporate into their block under construction. This block is then completed by a header, which contains in particular its hash and the identifier of previous block.

Since mining is (often) remunerated, the validation of a new block leads (but not necessarily) to a "competition" of miners among themselves. It is then possible that the chain of blocks has splits (two simultaneous versions coexisting) that occur. This is the case for example when two miners arrive at two different valid solutions for the same block at the same time and apart from each other. This case can also occur during the "update of all decentralized copies" because the replication of new blocks does not necessarily take the same time on all nodes (network latency for example). It is then possible that one of the nodes is not yet "synchronized" while a new block has just been validated and added.

The network is designed to resolve these splits in a short period of time, so that only one branch of the chain survives. The "longest" valid string is retained. The "length" of the chain does not refer to its number of blocks but to the most combined difficulty. It is a security designed to prevent forks.

Since the calculations needed to solve a block are intentionally energy-intensive and require more and more resources as the network grows, most miners are grouped into cooperatives. They then form a significant computing “power” and therefore increase their chances of seeing their blocks accepted and included in the Blockchain and being remunerated. As soon as a miner receives a block from another miner, he stops building the current block, which has almost no chance of being accepted. It eliminates it from its local waiting list all the transactions contained in the block it has just received, and begins to build a new block. This is how new blocks are produced and streamed through the network.

2.12 Smart Contracts

According of Nick Szabo in his “The idea of Smart Contracts”, Smart Contracts are Blockchain applications that express business logic associated with a transaction and execute on a Blockchain platform. Smart Contract code determines what transactions are recorded into the Blockchain and information they will contain. Through the use of smart contracts, many kinds of contractual clauses may be made partially or fully self-executing and self-enforcing.

Oracles provide a trusted service designed to supply external data to a smart contract or Blockchain system. Asset registers link digital currencies to other assets or records on top of a distributed ledger, according to interPARES Trust Terminology Project: “Key Blockchain Terms and Definitions” [19].

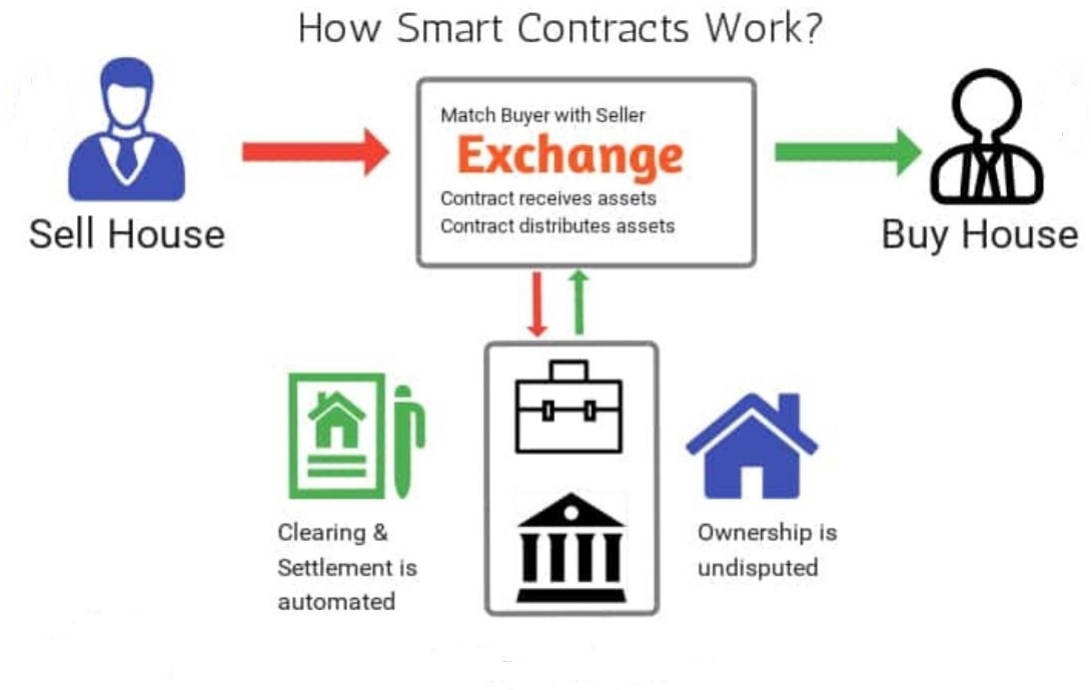

Figure 2.8: A smart contract in the Blockchain

2.13 Blockchain Consensus Mechanism

It is perfectly suited to deal with the "Problem of the Byzantine Generals"[7].

[7] **Problem of the Byzantine Generals:** is a game theory problem, which describes the difficulty decentralized parties

In Blockchain mode, consensus refers to the mechanism of guaranteeing that a transaction is not fraudulent and that a block is valid. The only way to bring out a global validation within the network is to obtain a "general vote" between all the stakeholders. The assumption made is that malicious users will always outnumber honest users. It is therefore important for network security that there are recognized mechanisms and/or rules, shared and validated by all, which make it possible to validate a transaction and then a block before it is added to the Blockchain, there are many methods of obtaining consensus on a Blockchain. The main ones are:

2.13.1 Proof Of Authority (PoA)

A proof of authority is the consensus mechanism of a private Blockchain that essentially gives a user, or a specific number of users, the right to mine all the blocks in the Blockchain.

2.13.2 Proof Of Stake (PoS)

Proof of Stake is a mechanism based on the amount of cryptocurrency purposely deposited by a user. This process is called minting and we then speak of forgers, the principle is as follows:

- A number of cryptocurrency holders are depositing a portion of their "assets" as part of the proof-of-stake mechanism. They then become "validators".
- When a new block is proposed for the addition of the Blockchain, a validator is selected, "randomly" among all the identified validators and is granted the right to create the next block and therefore to be paid.
- The selection of a validator is weighted according to the total amount of cryptocurrency (or token) they have deposited. For example, a validator

have in arriving at consensus without relying on a trusted central party.

with 10,000 “units” will have ten times more chance of being selected than a validator with 1,000 “units”.

- If this validator does not create the block within a given time interval, it is then “abandoned” and a second validator is selected, then a third and so on.

2.13.3 Proof of work (PoW)

Proof of Work is a block validation mechanism that relies on solving a complex crypto-mathematical problem. The resolution process is called mining and we talk about miners.

Figure 2.9: Proof of work kernel

As explained, there is a wide variety of methods, each with its advantages and disadvantages, its level of maturity and its quality of implementation. Their understanding is “essential” because they are an essential component for the proper functioning of the network. Let us quote a few more:

- Practical Bizantine Fault tolerance (PBFT)

- Proof of Hold (PoH)
- Proof of Use (PoU)
- Proof of Stake/Time (PoST)
- Proof of Minimum Aged Stake (PoMAS).

2.14 DApp (Decentralized Application)

decentralized application is an application connected to and using a Blockchain. It meets the following criteria:

- The application must be completely open (Open Source). It must operate autonomously and without an entity that controls the majority of its tokens. The application must be able to adapt its protocol in response to the improvements proposed at the level of the Blockchain it uses. However, all changes must be decided by consensus of its users.
- Application data and operation records should be stored crypto graphically in a decentralized Blockchain (public or not) to avoid any central point of failure.
- The use of a cryptographic token (crypto-currency Bitcoin, Ethereum or a native Token of its system) is necessary to access the application

2.15 The Blockchain network

The Blockchain network is the Internet network used as a peer-to-peer network. All network participants have the same status; no participant can claim greater legitimacy. Each participant is considered a peer with the others. The steps to run the network are as follows:

- Dissemination of all new transactions to all nodes to verify the history to be sure that the transactions are not used before and this operation is done by minors.
- Grouping of new transactions in a block of each node

- Each miner who includes the transaction in their block, Attempts to resolve proof of work with their block.
- We broadcast the proof of work to all the nodes of the network and each junction node learn from other nodes ask their neighbors for known.
- Once connected, the nodes only accept the block if all the transactions it contains are valid and have not already been passed. The nodes express their acceptance of the block by working on.
- The creation of next new block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the most secure and will continue to extend it. If two nodes simultaneously broadcast different versions of the next block, some nodes may receive one or the other first. In this case, the miners work on the first one they received, but save the other branch in case it gets longer. The tie will be broken when the next proof of work is found and a branch becomes longer; the nodes that were working on the other branch will then move to the longer one. New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will enter a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it requests it when it receives the next block and understands that it missed a block.

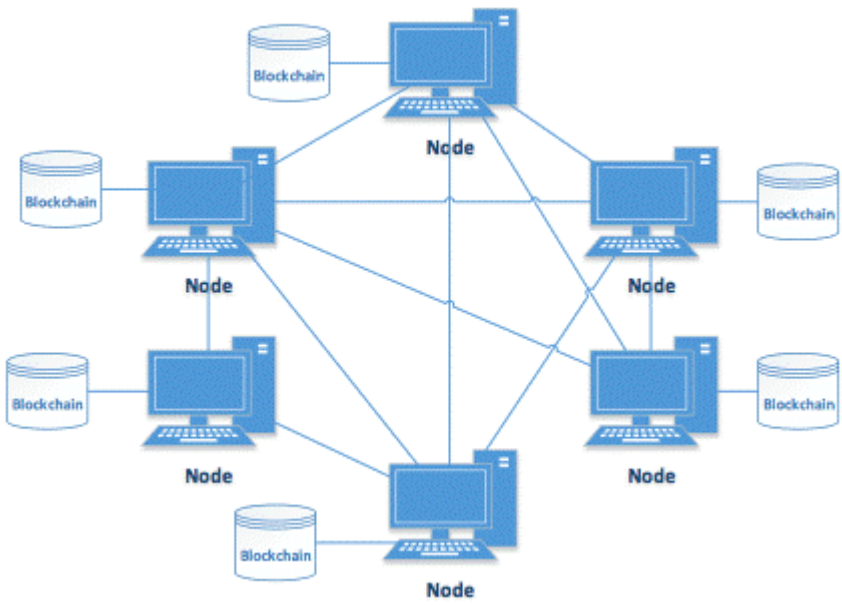

Figure 2.10: Blockchain network

2.16 Conclusion

In this chapter, we have studied the different stages and the technical process on which the Blockchain is based.

This study makes it possible to organize the exchanges of data on a distributed network (peer to peer), and secure the data by encryption, and involving the nodes of the network for the creation of new blocks of the chain.

The basic principle of a Blockchain is based on the notion of proof of work, and uses cryptographic techniques to verify the distinct holders of a collective registration system.

Chapter 3

Contribution

3.1 Project Objective

In this project, the objective is to implement the property verification system and to determine whether it can be applied by the Algerian government. Keeping digital copies of the digitally signed documents is an essential part of the system to verify the owner's identity and property security in today's world as property theft has increased. However, our state does not have a system for keeping digital copies of these documents.

Alternatively, this system may offer new solutions to combat corruption, since it allows the creation and storage of encrypted records that can be verified but cannot be altered. Through this system, entities will be able to protect themselves from fraud and corruption by protecting the transfer of ownership and commercial or administrative transactions. The architecture is distributed through a point-to-point network. The following sections will describe our application from a purely conceptual standpoint.

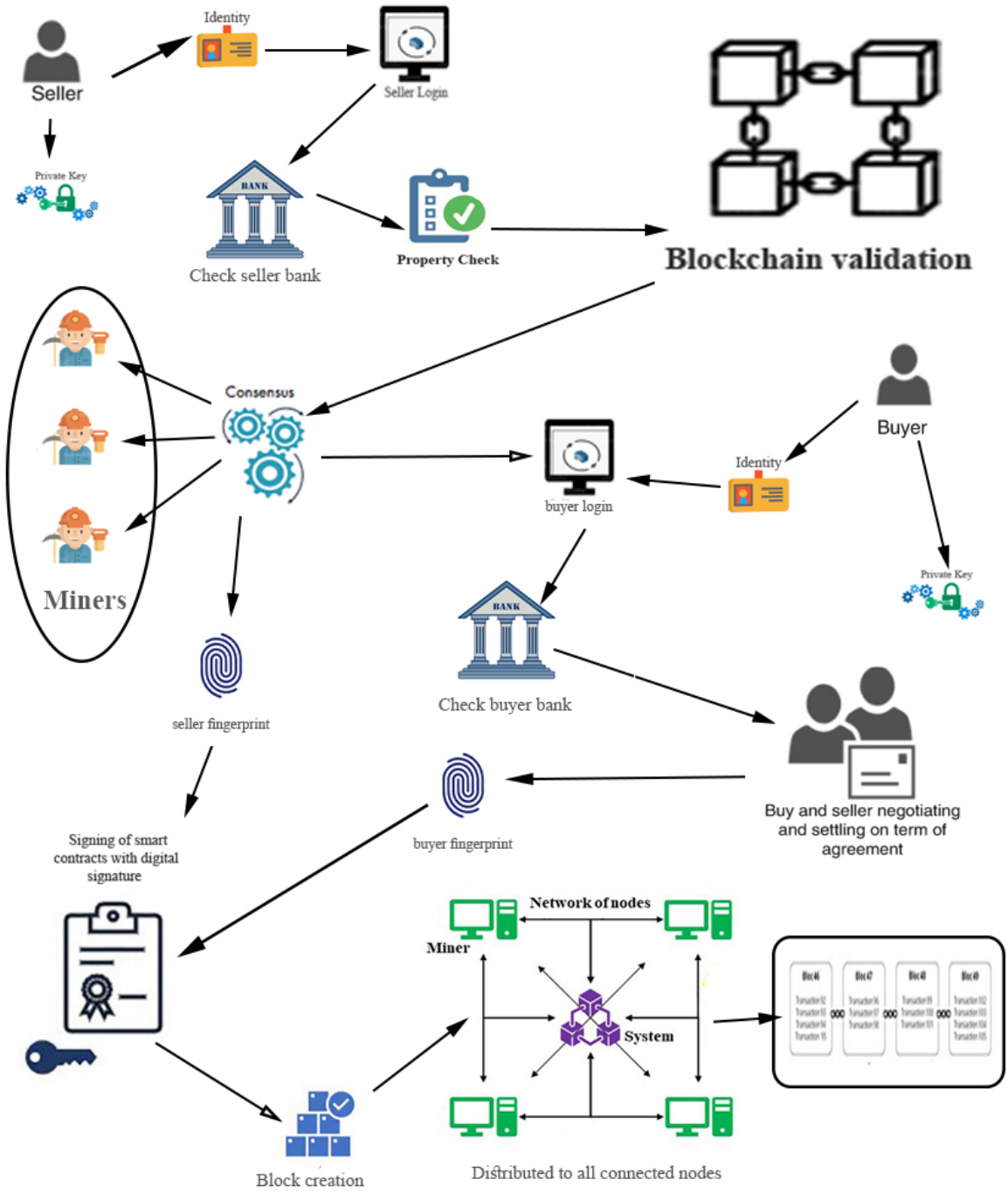

Figure 3.1: workflow of application architecture

3.2 The transition phase from the paper system to the electronic system:

As a starting point to creating the foundation for our future system, a move from paper to electronic is very important, as it consists of two phases:

3.2.1 Phase One: (Registration of land and owners)

The owner and the land are considered two prerequisites for achieving ownership, so first and foremost, a Blockchain system for the owners and another system for lands must be established and the information about them entered.

3.2.2 The second phase: (the phase of linking the land to the owners)

A process for linking lands with their owners and copying plans associated with them. After entering this information into the database, the digital data is reviewed and revised based on the information on paper records to ensure the validity of the entered data. A team of three investigators conducts the investigation. Once the first investigator has completed the review process and confirmed or canceled the record, the record is presented to a second investigator who does not know the result of the first investigator's review. In case the results are not similar, the record is presented to a third investigator with the same process.

After the process of reviewing and certifying all the data, the order is given to transfer it to the main block that contains the complete information of the properties. This basic block is contained within a series of other basic blocks for all the states of the country.

3.3 Components of the new system

- Customers Chain: Contains customer details, which are subsequently distributed to all states of the country.
- Property Chain: This Chain is divided into several other Chains according to the number of states of the country, where each state contains all the information related to its properties from the location on the map, area, address and several other information, the Chain is divided according to the states to facilitate the process of adding and searching later.
- Ownership chain: This chain is divided into two chains, which are as follows:
    1. Main chain: which contains the ownership details such as the property ID, the seller ID, the buyer ID, the signature of each of them, etc. This

chain is also the last step in the proposed process, where it can be referred to later in the consensus process to prove ownership.

2. Temporary chain: After the owner confirms the transfer of ownership, the transaction is added to this chain. After the verification and validation process is completed, it will move to the main chain.

- Smart Contract: It consists of the terms of ownership transfer that are determined by the contracting parties. The smart contract is divided into several types, such as a contract of sale, gift, inheritance, or other types.
- Black boxes: They are the external systems from which we derive the necessary information to verify the validity of the contract, such as the civil status system, the banking system, and the tax system, assuming that they work with Blockchain technology.

3.4 Operation phase (system activation)

After completing the transitional phase, the system is ready to begin moving the Algerian land registration process very close to a fully digital workflow based on self-executing contracts enforced by system participants.

3.4.1 Transaction process

The project's primary objective is to develop a secure, efficient, and reliable process for end-to-end land transfers using Blockchain. This update aims to reduce delays between signing a purchase contract and registering the title deed by reducing frequent checks and physical signatures. The system gathers all the necessary information before signing the ownership transfer agreement, allowing all parties to view the information before signing. This improved transparency leads to greater trust between the parties during the ownership transfer process.

3.4.1.1 Ownership transfer process

Several types of contracts exist, including sale contracts, gift contracts, inheritance contracts, and others. In order for the process of transferring ownership to

take place, both the owner and the person to whom it will be transferred must be present. In the first step, the owner logs into the system and selects the type of contract in order to verify that the transfer of ownership does not face any obstacles. Once this is completed, the property can be transferred without the need for an agent's intervention. If the seller still needs the agent, the agent is invited and can enter his e-key on the seller's behalf. After the owner performs the login process, a list of all his properties appears to him except for the properties that are being sold, where the system sends a request to all the main nodes in all the states of the country and checks whether this property is currently being sold or not, by searching in the temporary chains. When the list of properties appears, the owner selects the property to be sold or change its ownership, then the buyer or to whom the property will be transferred, whether he is a natural or legal person specified in the system, logs into the system that allows him to access the digital property account for evaluation. Since the real estate account contains all the necessary information, it is important to note that in the event of transferring ownership to a minor, the guardian will log into the system and add the person to his list of owing persons. Whether it's a gift or inheritance, a guardian can order ownership transfer on behalf of the minor with an identifier of the guardian.

Upon the two parties agreeing to the terms of the transfer of ownership, and after the new owner of the property certifies his initial approval with a digital signature, the smart contract is automatically activated, and the process of verifying and validating begins. As part of the process, the transaction is also added to the temporary chain list and all major nodes are notified immediately to avoid repeating the sale or transfer of ownership.

3.4.1.2 Validation of transactions

The process of approving and verifying transactions is considered to be the most important step in the system. In the event that the parties reach an agreement on the terms of the ownership transfer. As a start to the verification process, we will do the following:

- **Buyer's Bank Verification (in case of a sale):**

  It is necessary to verify that the buyer has an account with the bank that he specified earlier and also that he has the ability to pay the required amount by sending a request containing his ID. The request is sent with the understanding that the banking system operates using Blockchain technology. As previously mentioned, the banking system will not be the focus of this study, but rather treated as a black box.

  Following the verification of the request by the banking system, a response is sent to the system that sent the request. This response can be explained by one of two factors: either the buyer does not have an account with the bank, so they must choose another one. In either case, the buyer will be notified that the required amount is unavailable, resulting in a cancellation or postponement of the transaction.

- **Buyer's debts Verification (in case of a sale):**

  Following a positive response from the bank, the system sends a request to check the tax interests of whether the buyer has previous debts, which is dealt with as a black box if it is based on Blockchain technology. The land system, in this case, cancels or suspends the sale process, according to the final agreement between seller and buyer, if the debt is not paid automatically by the tax system. Alternatively, the buyer will have to pay the debt first.

- **Verification of land ownership :**

  One of the most pressing problems faced by a buyer is whether or not the seller or owner has the right to sell the property. Currently, land ownership information is stored on paper, and verification takes time and effort with the possibility of error very clear, as well as a fraud as it is possible to defraud land ownership.

  After completing the verification process of whether the buyer owns a bank account and has the required amount and has no debts as mentioned in the previous paragraph, the system sends a verification request containing the identifier of the owner and the land or property whose ownership is to be

changed to all the nodes related to it to participate in Consensus process, after receiving the verification request each node or (miner) searches its own Blockchain by landowner identifier and property identifier and validates the owner's ownership of the land.

3.4.1.3 How the nodes works (miners)

As soon as the miner receives the verification request accompanying the owner ID and land ID, the miner searches the Blockchain list by the owner ID, then searches the first search result by the land ID. It is important to keep in mind that during the search process, there may be more than one block that meets the search conditions, so in this case, the last block should be chosen based on the preservation date. If there is more than one block carrying the same data, you might want to refer to the modification procedure when saving incorrect information. Negative results are sent to the sender of the verification process in the event that the required block is not found. If the miner finds the required block, the data stored inside it is validated by going through the block hashing process and then comparing the result to the previous hash. When the comparison result is positive, this means that the ownership is accurate, and a positive result is sent back to the sender. Negative results in a comparison indicate that the data of this mine may have been tampered with. In this situation, the mine requests a renewal of the chain from the system central.

3.4.1.4 Receive the response from the validation process (consensus process)

The verification process has been completed and all nodes have been sent for a positive or negative response. Based on the number of nodes or astrologers participating in the consensus process, the system determines the percentage of positive responses. The validity of the land title is approved if the result is greater than or equal to (>=70 %). In the event the result is less than 70%, the sale will be canceled.

In order to validate that the smart contract meets all the necessary requirements. As soon as the process has been transferred from the temporary to the main chain, it is distributed to each of the 58 main nodes in each state. In this case, a new

block is added to each of the chains carrying information about land ownership. In the following step, the sub-chain will be updated and distributed to all nodes connected to the system at that time. The unconnected nodes are automatically updated once they are connected, as we will explain later.

3.4.2 Actors Communication process

As part of the system, there are the following actors:

- **Authority:** The authority owns the system and is responsible for creating land files, identifying owners, and encrypting keys, as well as managing and maintaining it. Each worker has his own account that is stored inside a SQL database that contains all the information. Each time a new account is created, a public key and private key are generated. To keep track of the users' work, the public key is stored inside the document whenever you transfer ownership.

- **The customer:** either he is the owner or the ownership will be transferred to him and he is a natural or legal person specified in the system, who can own a property and dispose of it individually or collectively with other people thanks to his identity file and his encryption key.

- **Miners:** A Blockchain is a distributed system connected in a point-to-point manner by powerful machines, and the miners themselves are the main and most important components that ensure the safety and security of the data. System's miners are most important for the following reasons:

  - Verify the identities of the landowners.
  - Verify the validity of the transfer of ownership and transactions
  - Create and verify chain blocks

- **Communication between Authority (Central Miner) and Miners:**

  In this regard, we used a direct connection established with both miners in a (client-server) mode, where clients need miners to identify themselves in the system.(see fig 3.2)

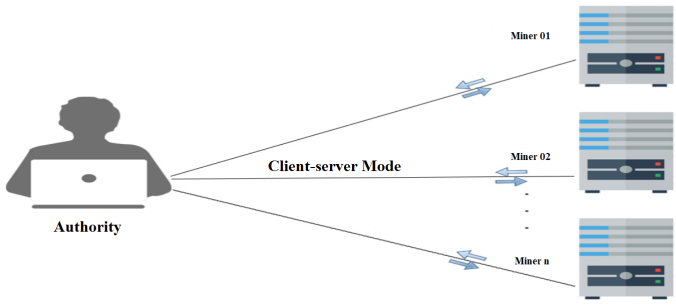

Figure 3.2: Communication between Authority and Miners

- **Communication between miners:**

  The connection between miners is established in a point-to-point (P2P) mode, where each client is a client and server at the same time in relation to other miners and they all perform the same actions and functions except for the central miner which has slightly different features from all miners other mines.

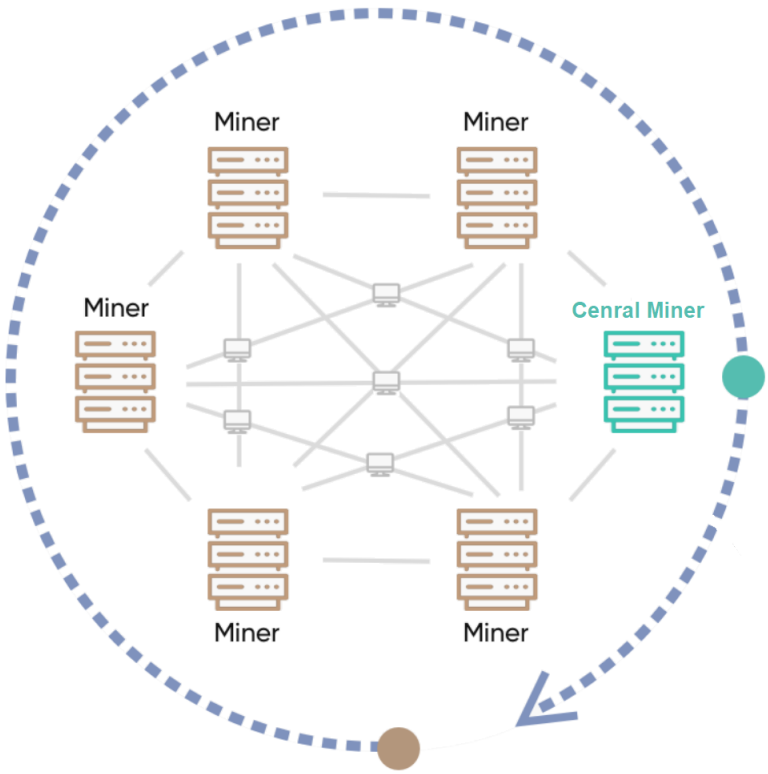

Figure 3.3: Communication between miners

3.5 Case study

In order for a project to succeed, it is imperative to start with the conception phase. Using modeling, these statements are expressed in a way that provides a

global overview without going into details about implementation. A UML model is presented here to illustrate how our solution is modeled. Activity diagrams and class diagrams were the most common tools we used.

3.5.1 The system specifications

Materials, products, or services must comply with a specification to be considered acceptable. The term "out of specification" may be applied to a material, product, or service that fails to meet one or more of the relevant specifications [30].

3.5.1.1 Functional specifications

Business processes into which a new IT product will need to intervene are described in functional specifications by a functional analyst. Its support for the tasks, interaction with the users, users, and stakeholders of other products, and the rules for interacting with them [30].
Login authentication can be performed without transmitting these identity files. In addition, it allows ownership to be transferred at any time without contacting a third party to confirm ownership.
The system must allow the authority to:

- generate encryption keys and create digital certificates and identity files.
- Add clients and their lands to the Blockchain.
- Consultation with the Blockchain
- Check the ownership of all completed transactions and consult with the parties involved.
- The system allows customers to be activated and deactivated.

3.5.1.2 Non-Functional specifications

This is a list of the specifications that characterize the system. Depending on the performance requirements, the type of device, or the type of design, these are the types. It is likely that these requirements will be related to implementation

constraints such as programming language, DBMS type, and operating system [30].

It is necessary to meet the following requirements before an extension can be granted:

- **Simplicity:** In addition to being used by a group of clients with different educational levels, the system must be easy to use to prevent any problems from occurring.
- **Availability:** It is imperative that the system is always available so that users can use it whenever they want.
- **Security:** The system contains personal information, so it must comply with the rules regarding the security of computer systems.
- **Performance:** A system's efficiency means that it should meet all the requirements of users optimally.

3.6 Modeling of functional specifications

It is considered necessary to represent functional specifications before beginning the implementation of each project in order to obtain a global view of the system requirements.

3.6.1 Class diagram

A class diagram is a diagram that is part of construction diagrams and contains a rich syntactic notation, making it one of the most commonly used UML diagrams. The diagram represents an object-oriented application's structure by showing the classes and their relationships [31].
the following diagram represents the entities of the system in more detail with its components and the associations between them:

3.6.2 Activity Diagram

The activity diagram describes the sequence of actions that make up a process, and provides a view of the system's behavior. In a way, activity diagrams are

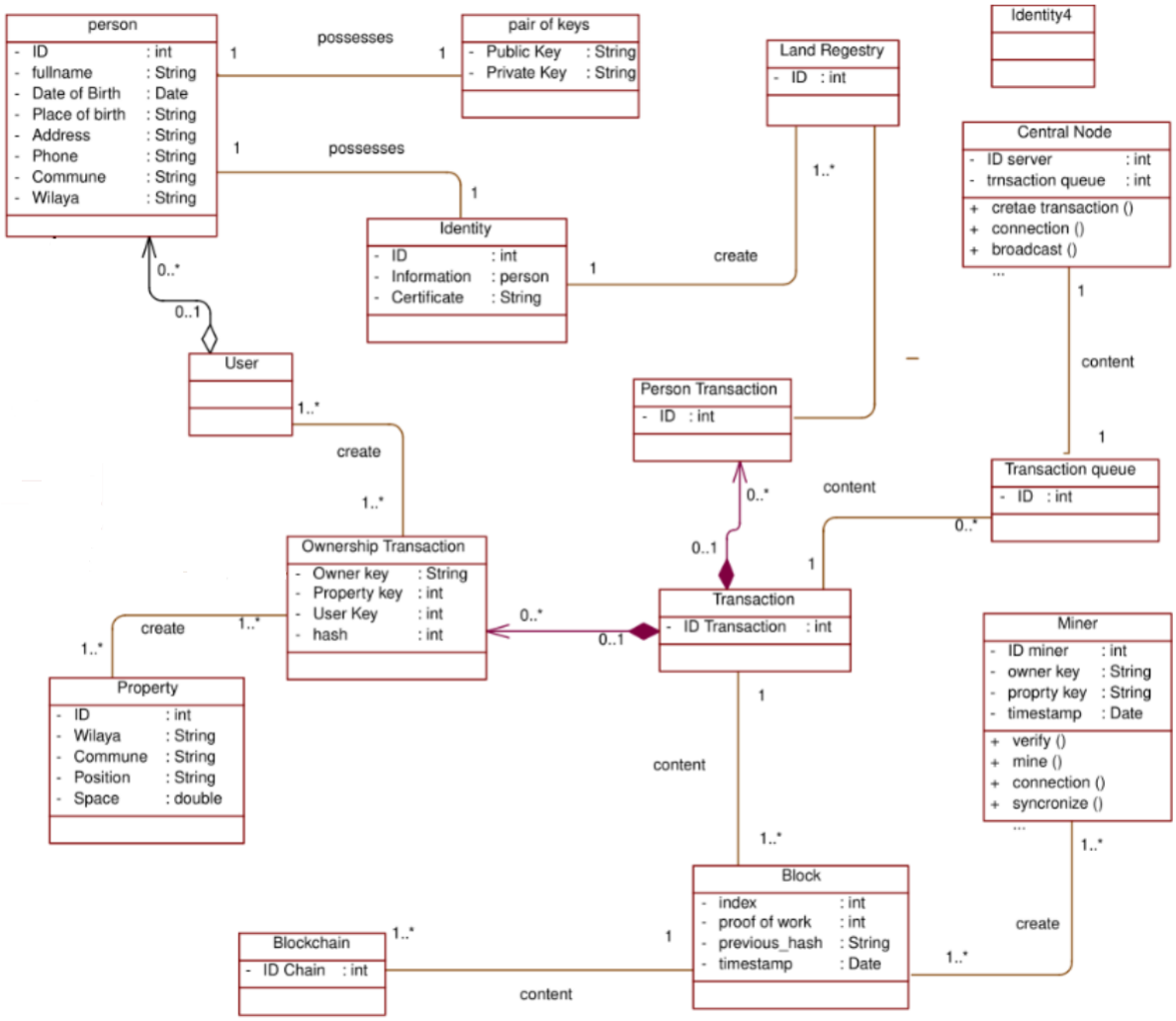

Figure 3.4: Class diagram.

similar to information processing flowcharts since they show the flow of actions in an activity. There are, however, no limits to the number of parallel flow diagrams and alternate flow diagrams that can be shown [14].

In this part we will represent the main use cases in the system using the activity diagram.

3.6.2.1 The creation of new owner

The first step to registering in the system is to create a user identity file. In this case, the client approaches a trusted third party authority that is considered by us to be a responsible authority. Providing the necessary documents proving the identity of the individual or entity, and registering the individual or entity with the system by creating a pair of keys and an identity file.

The following figure represents the activity diagram representing the interactions of the use case “creation of new owner”, or it represents in a clearer way how this process takes place:

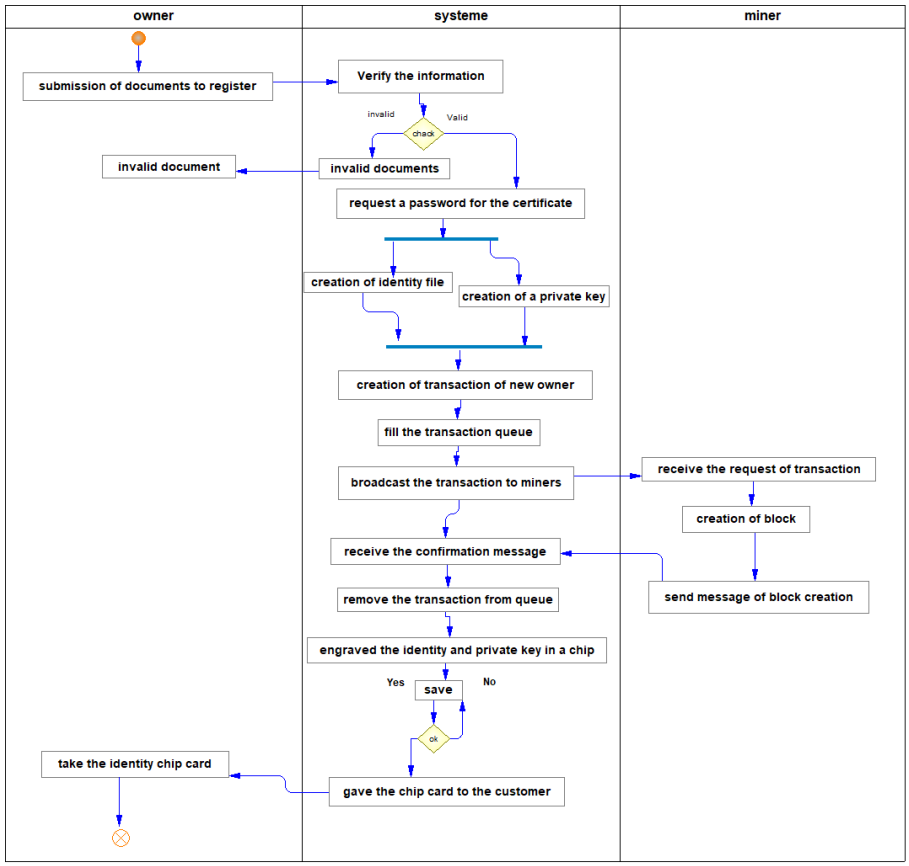

Figure 3.5: Creation of new owner

3.6.2.2 Description of ’Create an Identity’

The customer must first complete a registration process at the authority, accompanied by the necessary documents proving his identity. The following steps are followed after the documents have been validated.

1. The agent begins by checking the documents that prove the identity of the client.

2. He must then complete the Customer Information Form.

3. The customer is asked to choose a password for his signature certificate.

4. An encryption key is generated by the application with a length of 1024 bits.

5. It is then created and saved to the device an identity file encrypted with the system key, as well as a private key file.

6. A recording transaction is then created and stored in the "central miner" system.

7. The central miner receives this new transaction and stores it in the transaction queue.

8. The central miner then publishes the transaction to all miners connected to the system.

9. The miners begin the block creation process.

10. A confirmation message is sent by the miners to the central mine if a group of identities is created that can be multiple within the same block.

11. In order to create the identity, the central miner deletes the sent queue after receiving the confirmation. This confirmatory process is followed by the final process of creating the identity, which is the burning of this identity into a smart card.

12. It will then be possible for the customer to take out his smart card, which contains his identity file and his private key.

3.6.2.3 Connect to the system “Authentication Permissions”

A client’s account is associated with his account on the system without transferring any of his private keys or identity files over the network. Since we will only trust the entire system, this authentication process takes place after each node (miner) shares. Then, all miner participate in the client authentication process.

The following figure represents the activity diagram representing the use case interactions (connection to the system), or more clearly how this process occurs:

3.6.2.4 Description of “ authentication ”

The steps are described as follows:

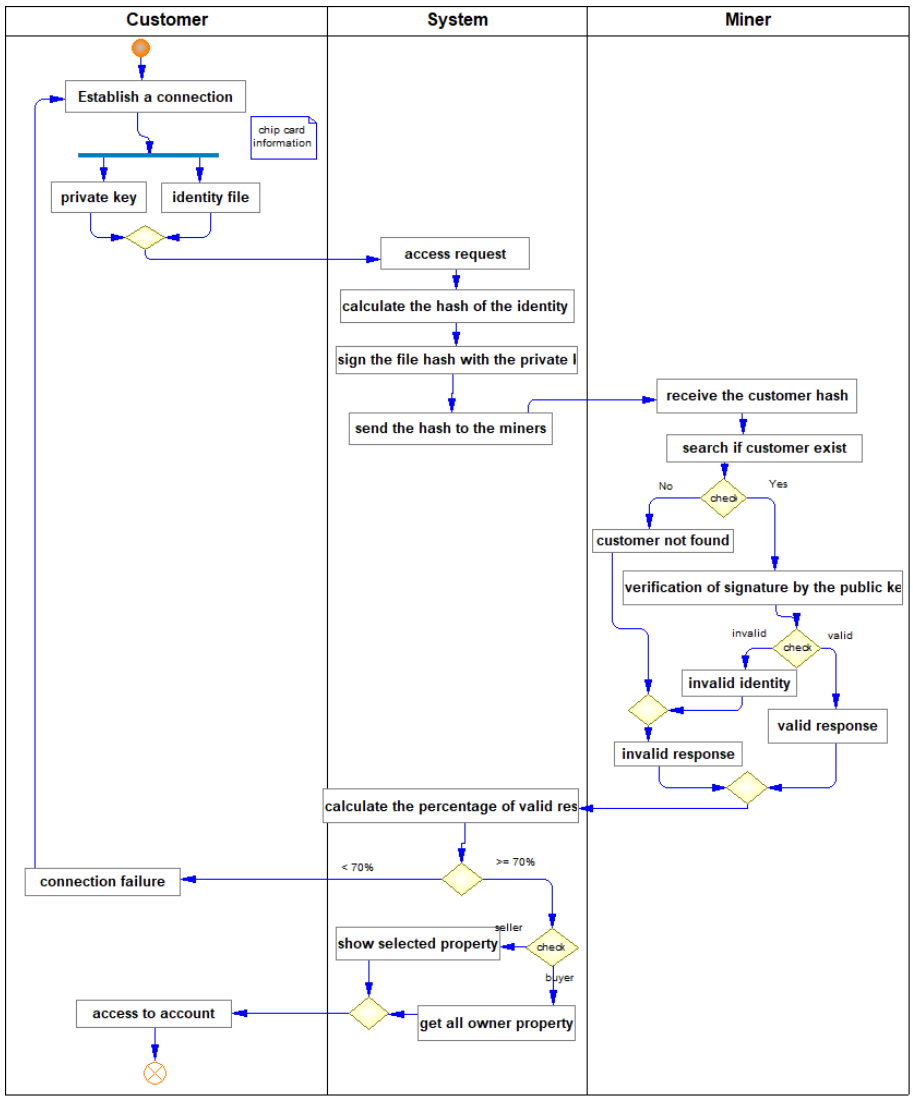

Figure 3.6: Authentication

1. By opening the client software, the client connects automatically to the central miner and gets access to the system. It establishes a connection with each of the connect miners that are active in the system after requesting a list of connected miners.

2. Once the smart card has been inserted into the reader, the customer must enter his ID, private key, and identity file manually to complete the process (in our app, this is done manually).

3. Once the hash of the identity file is calculated, the client application signs it with their private key and sends it along with the identifier to the miners.

4. Miners receive the information sent by the client and start searching if the identification number is present or not.

5. If the ID exists: It still checks if the client is in an active or disabled state in the system.
6. If the client is active, each miner verifies the hash signature sent by the client's public key with the hash in the transaction containing that client's information.
7. The miner returns a response to the system with the result of the identity verification.
8. According to the system, all miner identification messages are received and the percentage of positive responses is calculated regarding the number of minors. Clients whose percentages are greater than 70 percent (our offer) are allowed access to their accounts.
9. There is an automatic display of all the customer's properties provided by the program.

3.6.2.5 Ownership Transfer Process

A land record succeeds when all parties involved are trusting of one another. When records are evaluated as accurate, reliable and authentic, they can be considered trustworthy.

This diagram highlights the function of the land transfer process that can be adopted by the Republic of Algeria and suggests the implementation of a small pilot program that can be used as a proof of concept. The process can be illustrated as follows:

3.6.2.6 Text description 'Ownership Transfer Proces'

As a brief overview of the steps, here are the following:

1. First, the owner logs into the system, as was previously explained,you can see *diagram fig 3.7*.
2. After the owner confirms the login process, the system sends a list of all properties. It is necessary to choose the property that is to be sold or changed ownership.

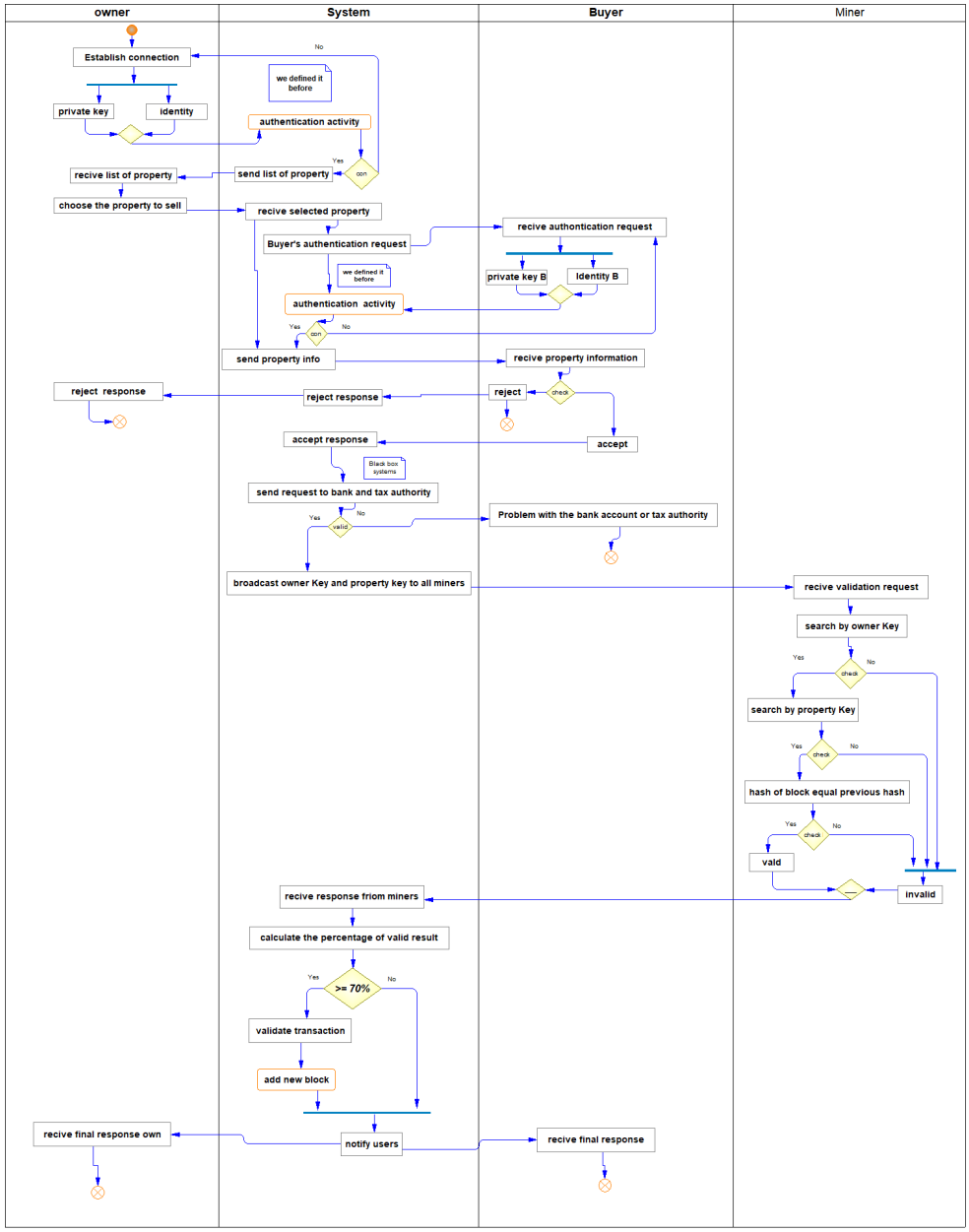

Figure 3.7: Ownership Transfer Process

3. The system immediately begins processing the property that the owner has selected. Upon receiving the login request, it sends it back to the buyer (in the same manner as before, but with a different user type).

4. Once the buyer's registration process is confirmed, the system sends the buyer all the information about the selected property for his approval. In order to avoid repeating the sale process, the buyer's approval of the new transaction is stored in the temporary chain immediately after it is approved by the buyer.

5. As part of the sale process, the system sends a verification request to the buyer's bank if it has the required amount and a second request to the tax

authority if the buyer is not in debt.

6. Upon receiving positive responses from the bank and the tax authority. System broadcasts to all miners or connected nodes a request containing the owner ID and property ID for verification of property ownership.

7. Each miner performs a search for the validity of the owner's existence after finding it. Make sure the property is owned by the correct person. The information stored in the block is then verified by calculating the hash value of the block and comparing it with the value stored in the next block (previous hash). Once the result is received, it is sent to the system.

8. Based on the values sent from the connected blocks, a percentage is calculated. Once the value reaches 70, a confirmation is sent to the system and ownership is transferred to the new owner. As an alternative, the regulator cancels the operation, and in either case, the transaction is removed from the temporary chain.

3.6.2.7 Activity diagram "Block creation"

In contrast to normal or shared databases managed by a central data manager. Blockchains have a unique and highly secure management system, which is dependent on all miners reaching a consensus.

In the following figure, we see the activity diagram representing how the use case is interacting (Creation of the block). In order to illustrate the process of the operation more clearly:

3.6.2.8 Description of 'Add new block'

After the system performs the process of consensus on the validity of the ownership ownership and the result is positive, the process of adding a block containing the new transaction begins as follows:

1. In the first step, the system retrieves the transaction from the queue and sends it to the mine that initiated the process, which is usually the same mine as the one that started it.

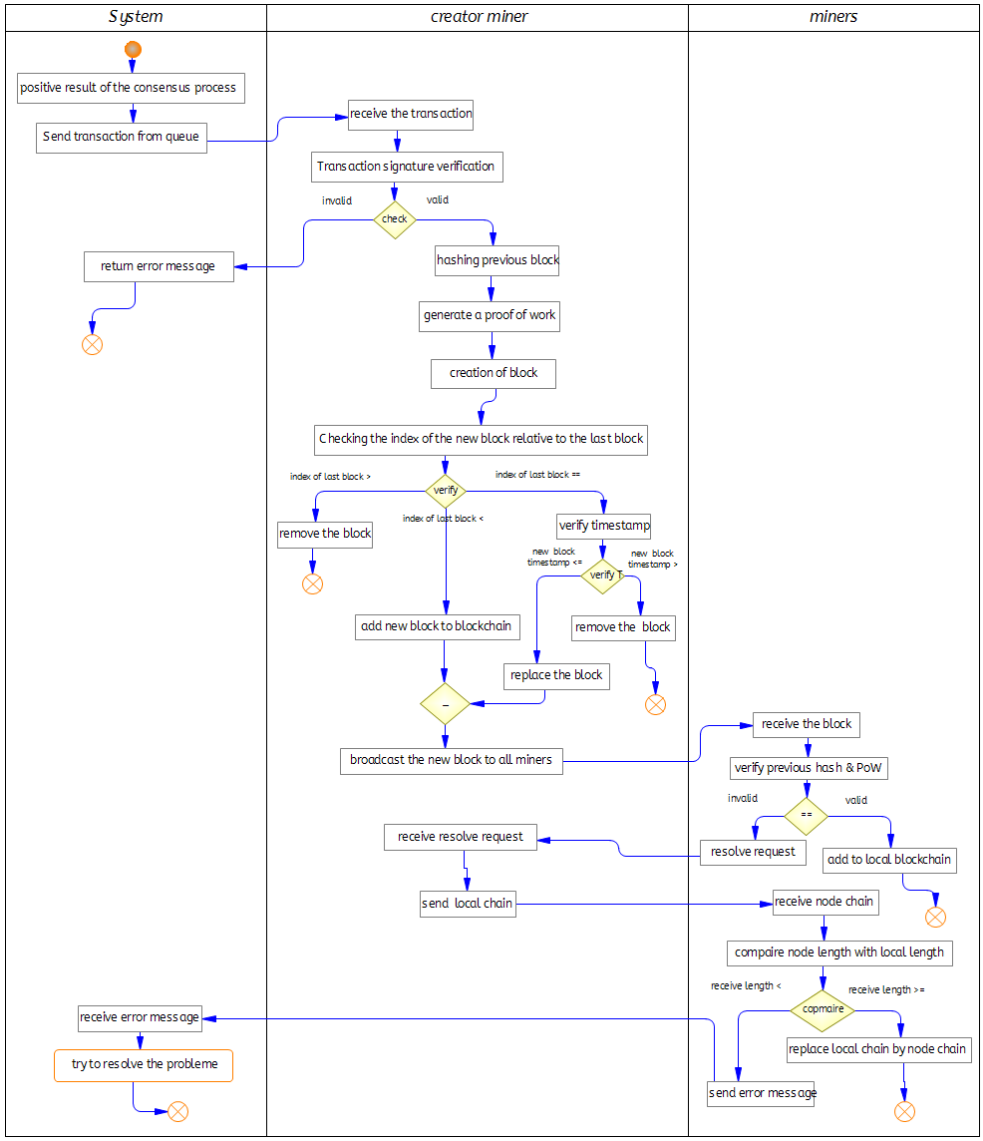

Figure 3.8: Add new block

2. It is necessary to validate the transaction signature. A signature is immediately placed in the transaction after the buyer agrees to own the property. A signature is used to ensure that the information in the smart contract has not been tampered with. An alert will be sent to the system and the smart contract will be completely canceled if the transaction information has been tampered with.

3. In the event that the signature is valid, we start creating the basic elements of the block. Firstly, we calculate the hash value of the previous block, then we calculate the proof of work for the block, and we add our transaction inside the block, making sure we don't forget to add the block's creation timestamp.

4. So as not to run into problems with the different blocks between miners, a block

verification procedure should be implemented before the block is added to the chain.

During the verification process, the following steps are taken:

- As long as the block that is being created has the same index as the last block in the chain, i.e. a block is received before the miner finishes creating the block, the miner will choose the block with the shortest creation time.
- When the newly created block has a higher index than the previous block in the chain, adding the block to the chain is done directly by the miner.
- In the event that the creator miner completes the block creation operation, the created block is broadcasted to all the other miners to verify it.

5. After the miner receives a block for adding, it calculates the hash value of the last block in its local string and compares it with the value stored in the new block (previous hash). After comparing the block against its local chain, the miner adds it to its local chain if the comparison is valid.

6. In the case where the comparison is not valid, the miner sends a solution request to the system. As soon as the system receives the request, it sends a copy of its chain to the miner. By comparing the length of the transmitted chain to its local chain, the miner calculates the length of the transmitted chain. In cases where the sent chain is longer than the local chain, the local chain will be replaced by the sent chain. If it is shorter, the problem will be reported to the system.

3.7 Conclusion

During this chapter, we were able to propose a conceptual solution describing the way to achieve the system to be developed. This process was used to model dynamic schema based on business and technical domains. and also introduced the coding of components from our solution. With this chapter, we've laid the groundwork for building the next step, which is the actual implementation and realization of our solution.

Chapter 4

Experiments and realization

> "If you tell people where to go,
> but not how to get there, you all be
> amazed at the results"
>
> *- George Patton*

4.1 Introduction

We'll now move on to the final section of our project, which will cover the big part and the subtitles of how we implement these models to create our solution to the problem. The implementation of our project requires a number of technology and development tools. We have chosen them on the basis of their characteristics that we consider suitable for our needs. We'll see our working environment, the software, and the IDE as we used them, then move on to languages, frameworks, and database systems, and finally, we'll conclude this chapter by introducing the main interfaces to our existing users.

4.2 Technologies used

Python is a multi-paradigm programming language. It promotes structured, object-oriented imperative programming. It has strong dynamic typing, automatic memory management by garbage collection and an exception handling system, it is thus similar to Perl, Ruby, Scheme, Smalltalk and Tcl.[21]

The Python language is placed under a free license close to the BSD license and works on most computer platforms, from supercomputers to central computers, from Windows to Unix via Linux and Mac OS, with Java or .NET. It is designed to optimize programmer productivity by offering high-level tools and an easy-to-use syntax. It is also appreciated by pedagogues who find in it a language where the syntax, clearly separated from low-level mechanisms, allows an easier initiation to the basic concepts of programming.[20]

JavaScript is a dynamic programming language that's used for web development, in web applications, for game development, and lots more. It allows you to implement dynamic features on web pages that cannot be done with only HTML and CSS.[15]

JavaScript allows users to interact with web pages. There are almost no limits to the things you can do with JavaScript, developers can use various JavaScript frameworks for developing and building web and mobile and desktop apps.

JavaScript frameworks are collections of JavaScript code libraries that provide developers with pre-written code to use for routine programming features and tasks—literally a framework to build websites or web applications around. Popular JavaScript front-end frameworks include React, React Native, Angular, Electron. Many companies use Node.js, a JavaScript runtime environment built on Google Chrome's JavaScript V8 engine. A few famous examples include Paypal, LinkedIn, Netflix, and Uber!.[16]

Electron is a free and open-source software framework developed and maintained by GitHub. The framework is designed to create desktop applications using web technologies (mainly HTML, CSS, and JavaScript, though other technologies such as frontend frameworks and Web Assembly are possible) which are rendered using a flavor of the Chromium browser engine, and a backend using the Node.js runtime environment. Additionally, it also uses various APIs to allow things such as native integration with Node services, and an Inter-process

communication module.[28]

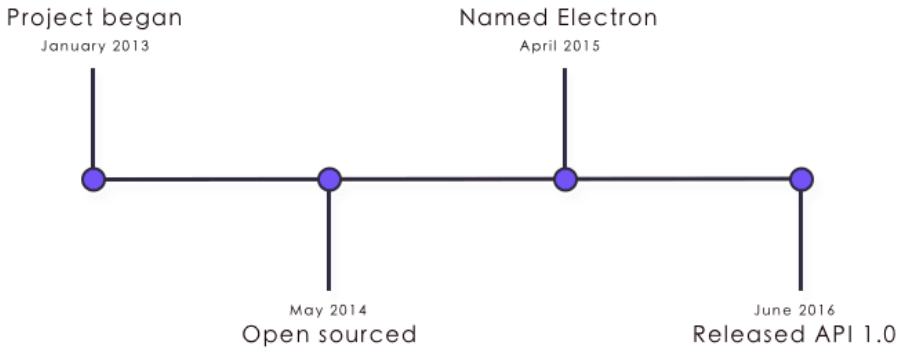

Figure 4.1: ElectronJS.

Assuming the above definition have solved your query on what is Electron.js, let's move onto its features.
Any web application you have written can run on ElectronJS, Similarly, any Node.JS application you write can utilize this technology.

Electron JS uses web technologies like simple HTML, CSS, and JavaScript. It does not require native skills unless you want to do something advanced. It can be designed for a single browser. Its file system belongs to Node.js APIs and works on Linux, Mac OS X, Windows.[9]

SQL is a standardized query language for requesting information from a database. The original version called SEQUEL (structured English query language) was designed by an IBM research center in 1974 and 1975. SQL was first introduced as a commercial database system in 1979 by Oracle Corporation.

Traditionally, SQL has been the preferred query language for database management systems running on minicomputers and mainframes. However, SQL is increasingly supported by database systems. Because it supports distributed databases (databases distributed across multiple computer systems). This allows multiple users on a local network to access the same database simultaneously.[6]

4.3 The tools used

- **Pycharm**

Pycharm is an integrated development environment used to program in Python.

It allows code analysis and contains a graphical debugger. It also allows unit test management, version control software integration, and supports web development with Django. Developed by the Czech company JetBrains, it is cross-platform software that works on Windows, Mac OS X and Linux. It is available in a professional edition, distributed under a proprietary license, and in a community edition distributed under an Apache license.[29]

- **VSCode (Visual Studio Code)**

Visual Studio Code has a high productivity code editor which, when combined with programming language services, gives you the power of an IDE and the speed of a text editor. In this topic, we'll first describe VS Code's language intelligence features (suggestions, parameter hints, smart code navigation) and then show the power of the core text editor.[12]

4.4 App Description

In this section we will present our application realized through some graphic interfaces and the output of each step of the work.

We have developed a graphical user interface that facilitates the implementation of the fundamental theoretical visions discussed at the beginning of this document.

4.4.1 Connection interface (Login)

Initially, the worker enters the program using his username and password,

choosing the state and municipality in which he works, and the program will auto-filter the information for that province after the login process.

The login process takes place through the SQL database (in our proposed

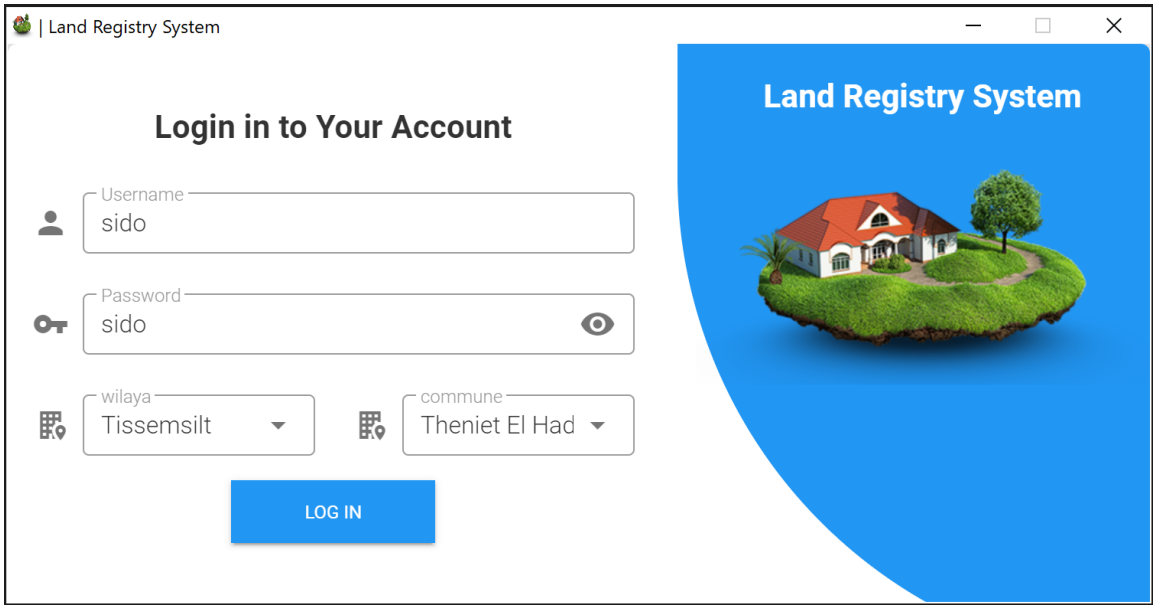

Figure 4.2: Connection interface (Login)

solution, a SQL-type database is used only to save the data of the system users). The user's public key (to be mentioned later) is saved inside the machine after the login process is verified, so that it can be used in every operation the worker performs.

4.4.2 List Of Menu

To facilitate the process of exploiting the content when using the software, we used the menu, as shown in the (fig 4.3)

- User Management (System users)
- Client Management (owners part)
- Property management
- Make Transactions (Change Ownership)
- Show Locations (Property Locations on the map)

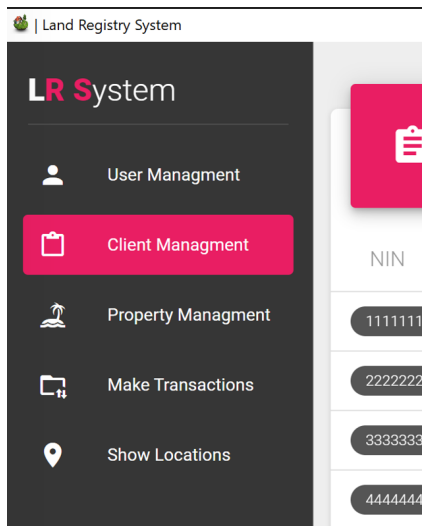

Figure 4.3: List Of Menu

4.4.3 User Management (System users)

In figure (4.4), you can see how the interface for adding and viewing all users for that region looks like. In the process of adding a new user, the central system creates two keys: a private key and a public key. The public key is used in all operations that this user performs in order to maintain traceability.
"'As the study revolves around the use of Blockchain technology to protect ownership transfers, the focus was not given to the users of the system"'

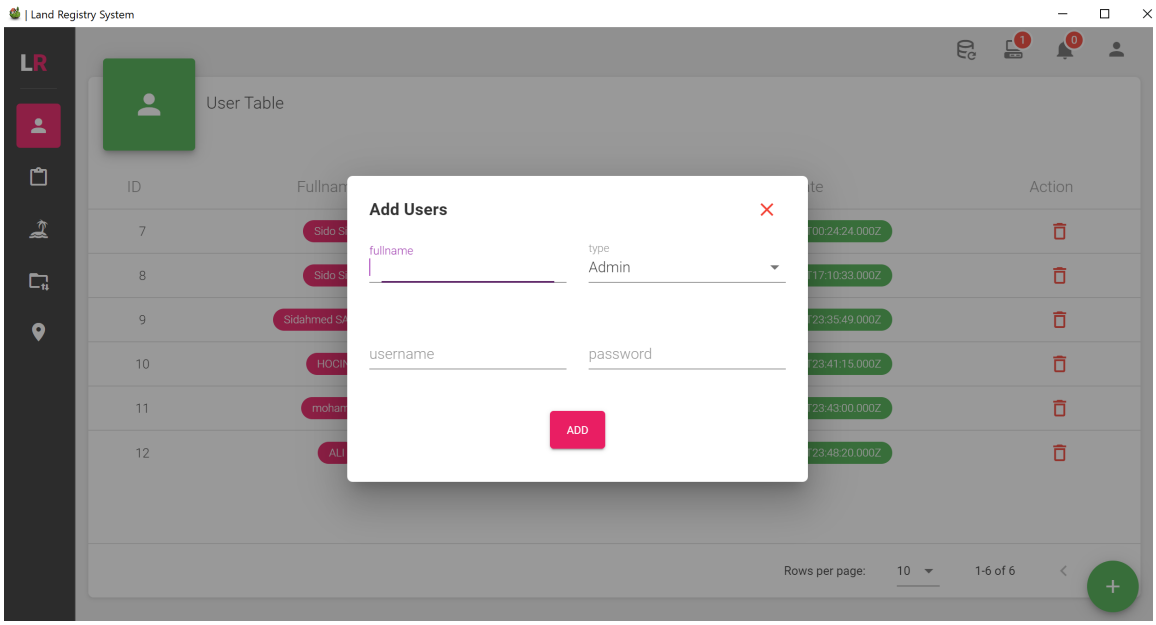

Figure 4.4: User Management (Add New User)

4.4.4 Client Management (owners part)

According to what was discussed in the previous chapter, the new system comprises several components. Chains are divided into three sections in the Blockchain file. Customer chains act as a container for all information about the owners in the country.

4.4.4.1 Add New Client

Figure (4.5) represents the interface for adding a new customer, which contains the national identity number (NIN), the full name of the person, his place of residence and some other information. The national identity number is taken from the national identification card as a unique number that represents the person to

be relied upon later.

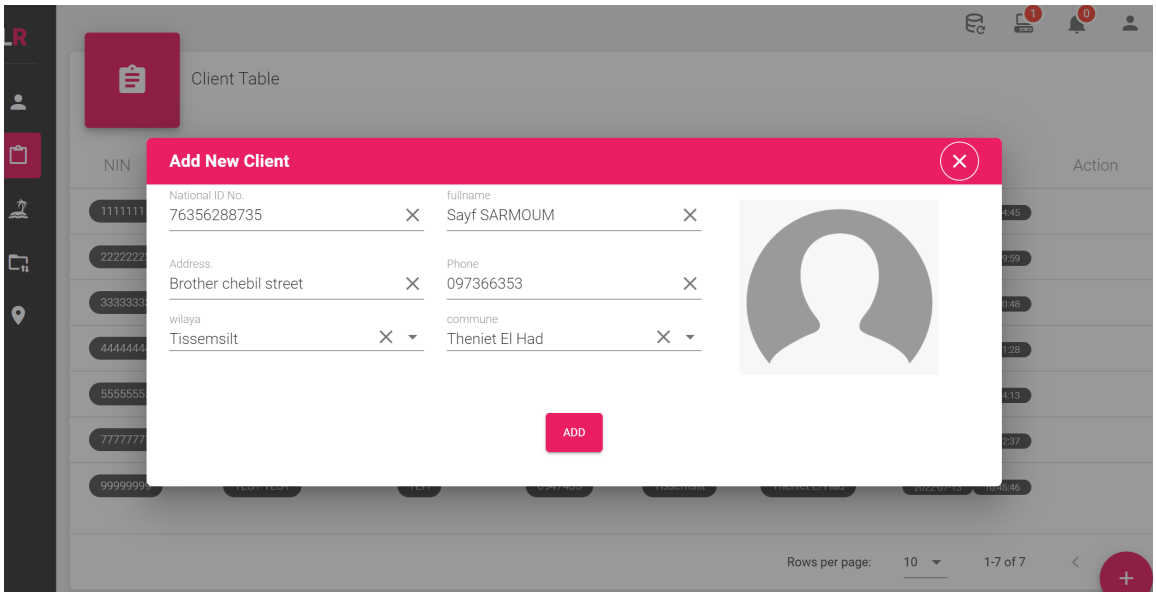

Figure 4.5: Client Management (Adding process)

With the click of the add button, an identity file and a pair of encryption keys are generated by the central system.

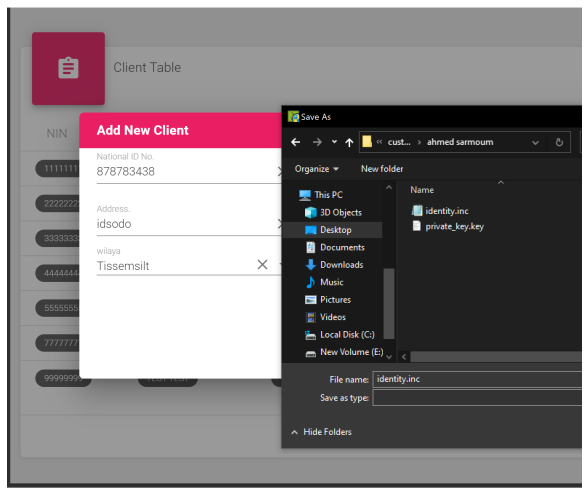

Figure 4.6: Generate identity and encryption keys

- Cryptographic key pair: To generate the client key pair we use RSA method, which is one of the most popular asymmetric encryption algorithms. That is, it is based on the principle of private and public keys, which only the recipient of the message is supposed to know in order to decrypt the message. What's important about this system is that you can't find the private key from the public key. One of the main advantages of RSA is that it encodes in blocks of characters, so it doesn't maintain the frequency of characters appearing [13].

  A pair of encryption keys is provided to each client in our system. It is a

private, personal, and secret key that only the client has access to. It is used to authenticate users in the system. As well as a public key that can be read by anyone and used to verify the identity of an individual, see fig (4.6).

- Identity file: It is a file that contains the necessary information for the client and is created by the authority and is encrypted using the AES method, which is the advanced encryption standard where we used [key length] - [block length]: 128-128 bits (in fact AES also supports variable block sizes, but This is not kept in the standard [25]).

  AES includes three block cipher algorithms: AES-128, AES-192, and AES-256, each of which encrypts and decrypts data in 128-bit blocks using 128, 192, and 256-bit encryption keys, respectively. Symmetric or secret key codes use the same key for encryption and decryption. So the sender and recipient must know and use the same secret key. All key lengths are sufficient to protect confidential information up to the "secret" level. On the other hand, information is at a "top secret" level.

  The file contains the following information:

  - The customer's first and last name.
  - Identification of the customer (NIN).
  - place of birth.
  - Telephone number
  - Client's address
  - Client's p12 SSL Certificate.

The following steps are followed after the identity file and encryption keys are created in order to create a block for this transaction:

- In order to work on the longest chain, we send a request to all connected or active nodes by sending a client chain length request.
- Add customer information with the previously created public key inside the new block.
- Confirm the validity and reliability of the chain by calculating the hash for each node and comparing it with the previous hash in the next node.

- After that, the hash of the last block is calculated and its value is placed in the new block as the previous hash.
- The block is then distributed to all connected nodes as a trusted and authentic block.

As is well known, hash functions are unique functions, which generates a fixed size output (called capacitors or fingerprint) that distinguishes the data provided. These functions are said to be one way because it is impossible to find the initial data of a fingerprint. The job is said to be "without collision" or "by injection" when it is very difficult to find two different sources that lead to the same result.

4.4.5 Property management

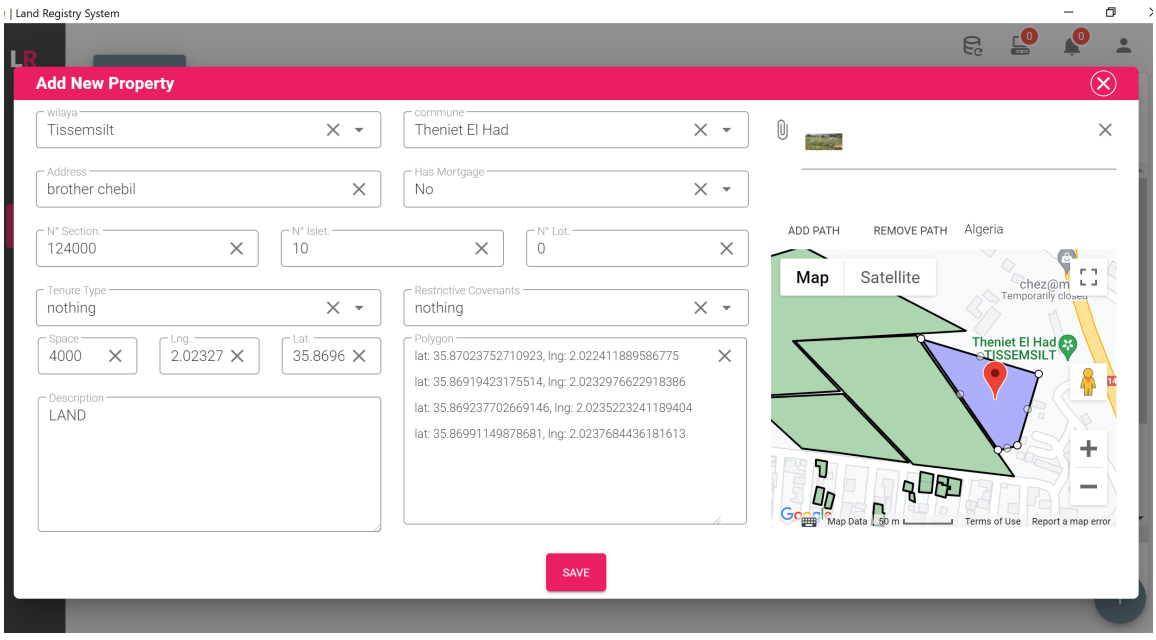

Figure 4.7: Property Management (Adding process)

In application of what was mentioned in the previous chapter about the steps of the transition process to the new system, especially with regard to adding property and lands to the distributed Blockchain file, Figure (4.7) illustrates the process and it is as follows:

The country and municipality are chosen in order to facilitate the process of adding to the Blockchain file, and the address, section and islet of the property is chosen for the possibility of identification and search later. In fact there is a lot

of information about the property that must be entered. The most important of which is the boundaries and coordinates of the property on the map.

After the area is determined on the map, the button add path is pressed to show the movable points to determine the boundaries of the property to be added as shown in the figure (4.8)

We can also see other immutable shapes (Shown in green) representing all the neighbors of the property to be added, Clicking on any of these shapes will give you all the information about that shape.

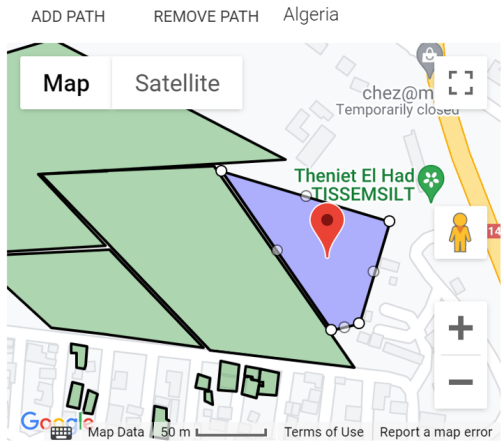

Figure 4.8: Polygon determination process

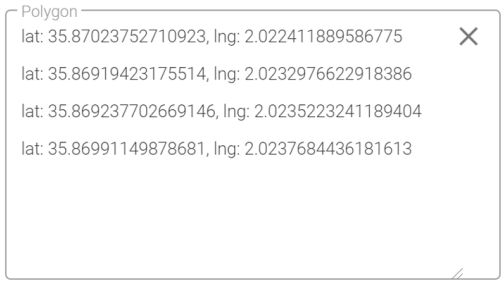

Figure 4.9: list of coordinates (Polygon)

In Figure (4.9), each point represents longitude and latitude, and by moving the lines we get the coordinates of the points on the map. As soon as we define the property, we get the final coordinate set.

Once you've completed all the required fields and clicked the save button, As soon as a new block is created, the system will add it as follows:

- A property chain length can be determined by sending a request to all nodes connected to the chain with the state and municipal numbers.
- Once the longest chain of blocks has been obtained. Like adding a new client, validating the integrity of the blocks and then hashing and building the new block are accomplished in the same manner.
- Nodes participating in the network receive the new block as soon as it is created.

4.4.6 Make Transactions (Change Ownership)

Ownership transfer is one of the most important steps to be completed in this project. Because this is where most frauds and deceptions take place. Additionally, the old system relied on paper systems that were unreliable, and other parties could have a corrupt background. It could take months for the process to be completed.

Taking ownership of a property has been divided into two parts, the first is for the owner, the second is for the new owner, which in our example represents the buyer.

4.4.6.1 Owner Login

As a starting point, we will discuss the following:

- the property owner enters his information using his identity file and his private key that were created previously. We assume the identity file and key are stored within a card. As shown in Figure (4.10), when the card is inserted into the automatic reader, it is loaded into its appropriate fields.
- Upon pressing the login button, the system decrypts the identity file (using the AES encryption method mentioned earlier) and retrieves all information about the owner. Also, we use the private key to create the digital signature of the property owner, which we use later during the confirmation process. The **RSASSA-PKCS1-v1-5**[1] algorithm was used to create it.
  A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very high confidence that the message was created by a known sender (authenticity), and that the message was not altered in transit (integrity) [27].
- Once the owner's information and his digital signature have been obtained,

[1] **RSASSA-PKCS1-v1-5** An old but still solid digital signature scheme based on RSA.

it is sent to all nodes or miners connected to the system, where each miner searches within the chain of customers and retrieve the owner's block. When the block has been hashed and the obtained value is compared to the value stored in the next block exactly the previous-block variable, the astrologer sends the number 1 if the comparison is correct, otherwise, the number 0 is sent.

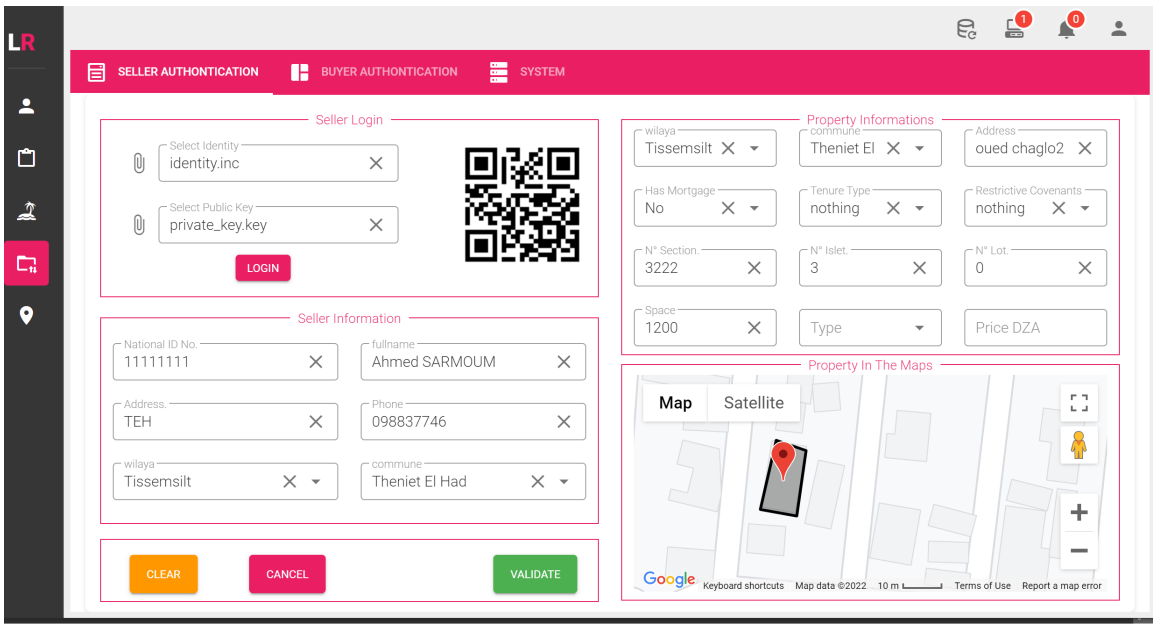

Figure 4.10: Log in to the system as a seller

- According to the previous chapter, the system calculates the percentage of positive consensus after all miners send the verification value. In the event of a positive consensus, the system sends a correction request to all negative nodes, then fetches all the properties of this owner and displays them to him as shown in the figure (4.10). If the result is negative, the owner is informed to repeat the process or to inform the authority once the problem has been resolved.

- The information is automatically displayed if you own just one property since it contains the owner's information, as well as the property information, and location on the map.

Owners who own multiple properties will see a list of all their properties so they can choose the one they would like to sell or change ownership of. see the fig (4.11). The owner then chooses the type of transaction (there are many types of transactions in this field that we did not mention all of them), but let's consider a sale as an example. As soon as the transaction type is chosen, the price of the property must be determined, and the bank receiving the transfer should be selected.

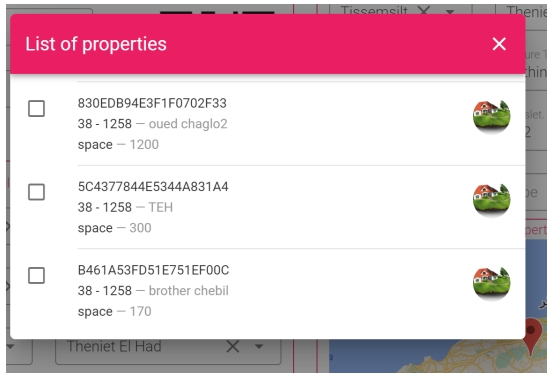

Figure 4.11: List of property

Once validate button is clicked, a unique serial number for new transaction is generated. the system creates a new block and adds this transaction to it, and then adds it to the temporary chain in the Blockchain file(which was discussed in the previous chapter), where the transaction contains the owner ID and his digital signature and this serial number, and is distributed to all related nodes.

Adding this transaction to the temporary chain and passing it along to all connected miners ensures that the property will not be sold twice, as it is in the current system. The property is locked once it has been selected, to prevent it from being exploited thereafter until the ownership is changed or the process is halted.

4.4.6.2 Buyer Login

According to the proposed future of the system, the QRCode or serial number would be sent to the buyer once the owner confirms the request. At present, the serial number of a transaction appears in the buyer's login interface see fig (4.12).

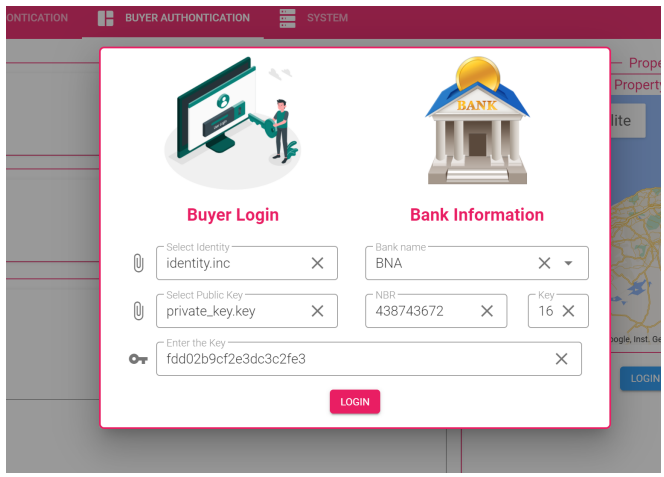

Figure 4.12: Buyer login interface

By inserting his card containing the identity file and public key,

the buyer also chooses the bank
through which he will make the payment. The serial number will be copied into that field if the entry process is immediate after the seller confirms. If not, it will be retrieved from the QRCode of the addressee or obtained from the administration. The process of verification is similar to that of verifying the owner's information except for the step of obtaining the property.

As soon as the login process is successful, the system saves the digital signature of the buyer and searches the temporary chain in the distributed Blockchain file, retrieving all owner, property and transaction information.

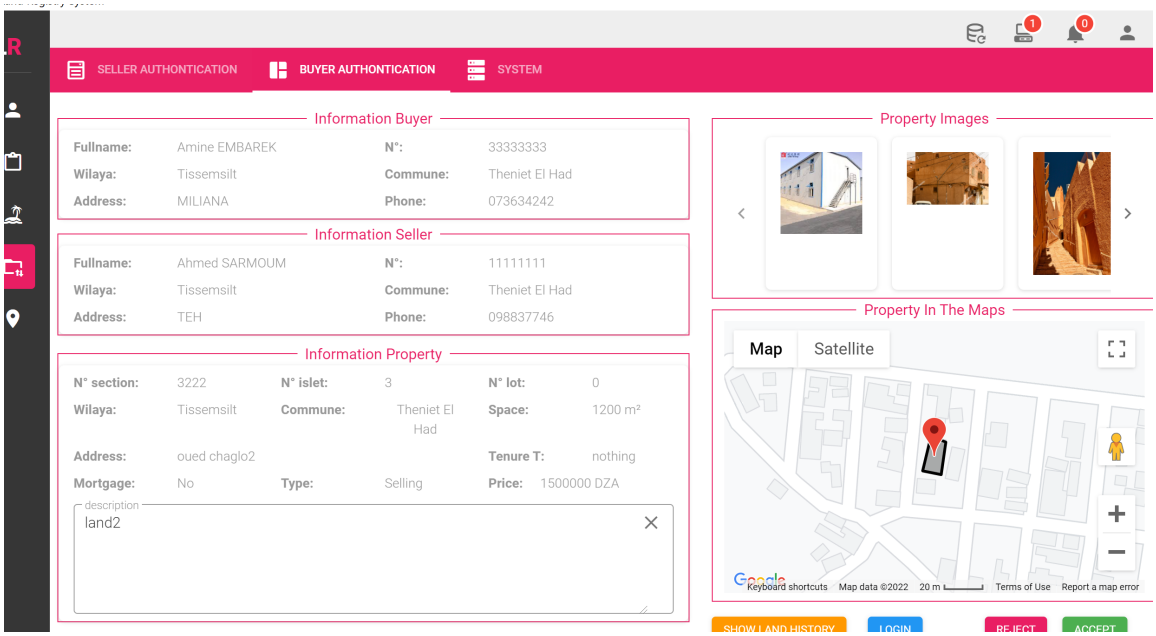

Figure 4.13: Display all transaction information

Figure (4.13) is a screenshot of the interface showing all reliable information, including photos of the property if available, its location on the map, as well as its history.

After pressing the Accept button, the system will contact the buyer's bank and verify that they have the required amount (as mentioned in the previous chapter). In the distributed blockchain file, after completing the bank verification process and transferring the money to the owner's bank, the transaction is transferred from the temporary chain to the ownership chain, the digital signature of the buyer is added to it, and a new block is created for this transaction. It is then distributed to all miners. In order to enable the new owner to exploit it, the

transaction is deleted from the temporary chain.

4.4.7 Show Locations (Property Locations on the map)

All the property polygons from the blockchain file were fetched and displayed on the map, where we can click on any property to display the name, surname, national ID no (NIN), and unique serial number of the property and its area, as well as the neighbors throughout the map to facilitate its description see Fig (4.14). As mentioned previously, we used JavaScript to build the Frontend so that we can make the application special to the desktop as we can make it a web application, by using this feature we can display this real estate map to the public while hiding some sensitive information so that citizens can take the necessary and reliable information without having to resort to the administration.

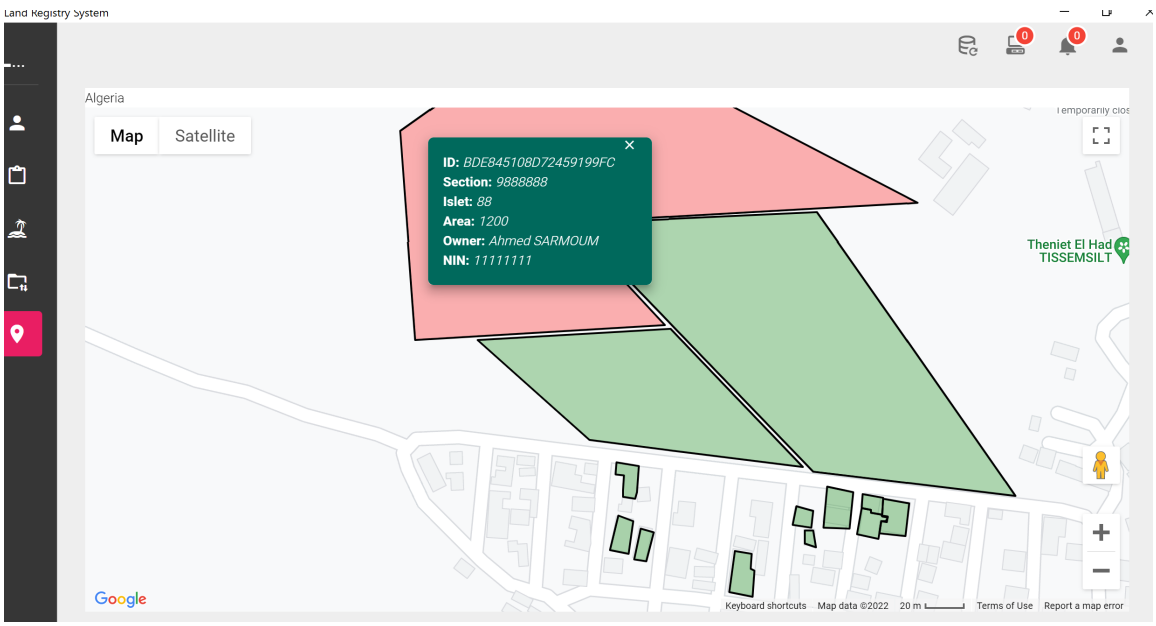

Figure 4.14: Property Locations on the map

4.5 Conclusion

‘ This chapter covers all the steps we took to get to the final Blockchain file (land book secured by the Blockchain), as well as our work environment. Our next step was to present our application architecture, which helped us to get a better understanding of how our application was implemented.

General Conclusion

Through the use of Blockchain technology, the aim of this end-of-study report is to establish a reliable method of validating transactions during ownership transfers, where the primary objective is to ensure data integrity and ensure completion of transactions..

As we have seen, Blockchain technology is not just for electronic money, but can also be used for verification of property transfer transactions.

Understanding how electronic money works requires understanding the working mechanism of this new technology. With Blockchain technology, each system can determine its own functions and mechanisms, while respecting the fundamental principles of the technology. At the same time, consensus is the most important characteristic of decision-making, As part of each process, all elements of the system contribute to the validation of the information to provide an answer, while ensuring the answers of the majority of the elements of the system to make a decision.

The advantages and disadvantages of each solution vary depending on the use case. With Blockchain integrated into the land registry system, users will have greater protection of their privacy. As the only secure system is able to access the computer chain through which the connected objects communicate. It is possible to track the exchange of data between devices and property exchange services through Blockchain technology by recording the unique history of each device.

Among them are land and property transactions that require verification in different areas. As a result of this development, the property transfer system will be highly protected, allowing for much easier process control. Lastly, even though our solution is not perfect, using technology like Blockchain to increase the transparency of the ownership transfer will improve its reliability. In addition, it will reduce tedious, manual and repetitive tasks for clients, authorities and all other stakeholders provided that the encryption keys used are under the control of the user.

Bibliography

[1] *The domain – the ENC cadastre*.

[2] *Larousse dictionary "etymological"*.

[3] Kairos Future. 2017. "blockchain and distributed ledgers as trusted record-keeping systems: An archival theoretic evaluation framework".

[4] Kairos Future. 2017. "the land registry in the blockchain – a testbed". `https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf`.

[5] Maurice BARBIERI and Dr. Dominik GASSEN. World bank conference on land and poverty. In *The World Bank - Washington DC*, pages 3–4, 2017.

[6] Vangie Beal. Sql-structured query language,. `https://www.webopedia.com/definitions/sql/`.

[7] Bitcoin. Blockchain history.

[8] R. Bowden, H.P. Keeler, A.E. Krzesinski, and P.G. Taylor. Block arrivals in the bitcoin blockchain. 2018.

[9] Brainhub. Key features of electronjs. `https://brainhub.eu/library/what-is-electron-js`.

[10] Fran Casino, Thomas K. Dasaklis, and Constantinos Patsakis. A systematic literature review of blockchain-based applications: Current status, classification and open issues. 2019.

[11] Raffaele Fabio Ciriello, Roman Beck, and Jason Bennett Thatcher. The paradoxical effects of blockchain technology on social networking practices. 2018.

[12] code.visualstudio. Visual studio code. `https://code.visualstudio.com/docs/editor/editingevolved`.

[13] comparitech. What is rsa encryption and how does it work? https://www.comparitech.com/blog/information-security/rsa-encryption/.

[14] Developpez.com. Uml 2 :de l'apprentissage à la pratique. https://laurent-audibert.developpez.com/Cours-UML/?page=diagramme-activites.

[15] freecodecamp.org. What is javascript? a definition of the js programming language. https://www.freecodecamp.org/news/what-is-javascript-definition-of-js/.

[16] hackreactor.com. What is javascript used for? https://www.hackreactor.com/blog/what-is-javascript-used-for.

[17] Toufique Imam, Yamin Arafat, Shaikh Akib Shahriyar, and Kazi Saeed Alam. Doc-block: A blockchain based authentication system for digital documents. In *Conference: 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, 2021.

[18] 2016 L. Coleman. "georgia expands project to secure land titles on the bitcoin blockchain" cryptocoin news. https://www.cryptocoinsnews.com/republic-of-georgia-expands-projecttosecure-land-titles-on-the/bitcoin-blockchain/.

[19] Victoria L. Lemieux. Blockchain and distributed ledgers as trusted record-keeping systems: An archival theoretic evaluation framework. 2017.

[20] leparisien.fr. Python language. https://dictionnaire.sensagent.leparisien.fr/PYTHON%20LANGAGE/en-en/.

[21] limswiki.org. Python (programming language). https://www.limswiki.org/index.php/Python_(programming_language).

[22] Pierre-Marie Lore. *Blockchain : évolution ou révolution des contrats en France ?* France.

[23] Nakamoto. Source: Bitcoin "a peer-to-peer electronic cash system", nakamoto 2008. https://shorturl.at/arsU8.

[24] Peter B. Nichol. Why swarm intelligence enhances business and bitcoin.

[25] securiteinfo. Aes : Advanced encryption standard. https://www.securiteinfo.com/cryptographie/aes.shtml.

[26] Rakesh Shrestha, Rojeena Bajracharya, Anish P. Shrestha, and Seung Yeob Nam. A new type of blockchain for secure message exchange in vanet. page 179, 2020.

[27] Wikipedia. Digital signature. https://en.wikipedia.org/wiki/Digital_signature.

[28] Wikipedia. Electron (software framework). https://en.wikipedia.org/wiki/Electron_(software_framework).

[29] Wikipedia. Pycharm. https://fr.wikipedia.org/wiki/PyCharmS.

[30] Wikipedia. Specification (technical standard). https://en.wikipedia.org/wiki/Specification_(technical_standard).

[31] Wikipedia. Uml modeling: The class diagram(2019, may 12). https://en.wikipedia.org/wiki/Specification_(technical_standard).