BABEŞ BOLYAI UNIVERSITY, CLUJ NAPOCA, ROMÂNIA

FACULTY OF MATHEMATICS AND COMPUTER SCIENCE

Blockchain in Real Estate

– Diploma thesis –

Gabor Petru Andrei

Supervisor: Crăciun Mihai Florin Gabriel

2022

Abstract

The underlying layer of cryptocurrencies, blockchain technology, is one of the most ambitious technology after the internet, as its adoption is growing at the moment. This thesis studies the importance of blockchain technology in real estate industry and highlights the needs for a fusion, along with the current technological and economic developments as the facilitators of adaptation between them.

Personally, I am excited about the many Internet of Things and Big Data technologies that are now affecting the real estate industry. Blockchain technology is significantly more advanced than what is now available. It has the potential to disrupt the real estate sector, which makes it a fascinating and timely subject to research.

This report also contains important information regarding this new technology and its implications for the large bureaucratic framework of any smart government service. The study is focused on an example of real estate trading.

Contents

1 Introduction

"We have elected to put our money and faith in a mathematical framework that is free of politics and human error."

(Tyler Winklevoss) [KOS18]

The twenty-first century is now undergoing a technological revolution. Everything began to change and shift into a technology trend around us. The technological environment, in its numerous forms, underpins energy, economics, services, security, transportation, finance, administration, and other elements of life. People are being encouraged to embrace new technologies as a result of the need for more modernization in all parts of life. The usage of a remote control to control various household appliances has developed to the use of audio notes to provide advice. Over the previous decade, the emergence and discovery of technologies such as AR and IoT has accelerated, and now Blockchain has been added to the mix.

The whole market is seeing a technological shift, with multiple marketplaces in need of technology that can speed up various operations while also increasing market safety and transparency. The real estate market is one of these marketplaces, and it is vital to a country's overall well-being. In addition, real estate crises are frequently connected to market inefficiencies, such as illiquid markets, a lack of transparency, high transaction costs, human biases, and lengthy transaction procedures.

The typical transaction procedure begins with the property owner opting to sell and contacting a real estate broker in most circumstances. The broker appraises the property and works out an appropriate asking price with the seller. When it's decided, the broker will begin marketing the property and looking for a buyer. When a possible buyer is identified, the process of evaluating and negotiating begins. When a buyer and seller agree on a price, they normally draft a contract and complete the transaction. The buyer must normally register the transaction price to a government agency, while the broker reports it to a specialized realtor database. [DC17]

Figure 1: Steps for selling a property [Blo]

The system is stagnant for various reasons, the most important of which being the repetitive process of verifying data. Many of the paperwork must be signed on paper and sent via the postal service. Manual methods are required for document validation. Because of the large number of signed papers, errors sometimes arise and must be addressed. When all of these factors are combined, the process becomes slow and inefficient. Higher transaction costs arise as a result of the time-consuming process.

Many of these unproductive operations might be decreased or eliminated with blockchain technology:

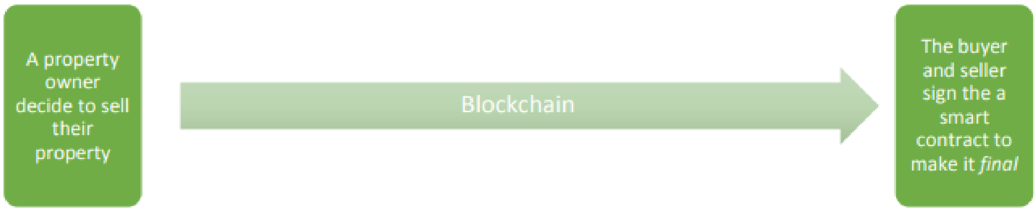


Figure 2: Selling equity using blockchain technology

In comparison to today's technology, blockchain technology is far more secure. Fraud and missing papers are impossible or minimized with this new technology, and the entire transaction procedure might be greatly shortened.

But the outcome of implementing new technologies is not always clear and could affect far more areas than imagined. The real estate sector is vital to the economy as a whole, and it should not be put at unnecessary risk while implementing new technology. It is not highly regulated, so it might take some years until this will really be a regulated solution.

2 Real Estate Market

Real estate is land and the buildings on it, as well as natural resources such as crops, minerals, and water; immovable property of this sort; an interest in this piece of real property, buildings, or dwellings in general. Vehicles, yachts, jewels, furniture, equipment, and agricultural rolling stock are examples of personal property that are not permanently tied to the land. Global real estate is the largest repository of wealth, with about 280 trillion dollars in assets. Real estate, after stocks and gold, is the third fastest growing asset class in 2017, with an increase of 8% in value. In global real estate, however, there are common interests.

If the financial system is weak and too tightly tied to the country's real estate industry, a financial crisis frequently results from a real estate crisis. As a result, a well-functioning real estate market is critical for a country's economic development.

People often use the terms land, real property, and real estate interchangeably, but there are some distinctions:

- The term "land" refers to the earth's surface from the core to the airspace above, including trees, minerals, and water.

- The collection of interests, benefits, and rights that come with owning real estate—one of the two primary classes of property—is the set of interests, advantages, and rights that come with owning real estate.

- The term "real estate" refers to the land as well as any permanent man-made structures such as houses and other structures.

As the definition says, real estate includes the physical surface of the land, what lies above and below it, what is permanently attached to it, plus all the rights of ownership—including the right to possess, sell, lease, and enjoy the land. Real property shouldn't be confused with personal property, which encompasses all property that doesn't fit the definition of real property. [CHE21] One of the main characteristics of personal property is that it's movable.

Physical characteristics:

- Uniqueness: There can't be two identical plots of land. Despite their similarities, each parcel is geographically distinct.

- Immobility: While some land can be removed and the terrain modified, the geographic position of any piece of property can never be changed..

- Indestructibility: Land is durable and permanent.

2.1 Real Estate Transparency

A transparent real estate market is organized, open and operates with available information in a reliable manner between parts. Despite the fact that the term "transparency" is widely used in the real estate industry, it is not properly defined. Tough transparency in economic science is seen as information shared equivalent of the participants on the market, the opposite of transparency can be interpreted as information asymmetry. To achieve a successful investment in real estate, a certain level of transparency on the market is essential. There is an ongoing change towards an improved transparency, which has occurred during the last decade in several countries. The need for market information has expanded significantly as a result of greater globalization and the associated dispersion of transactions and corporate activity.

Because real estate openness has the potential to minimize property market speculation, which can lead to property bubbles or other negative effects on national economies, decision-makers should assess the progress in transparency (governments and big companies).

The Global Real Estate Transparency Index (GRETI) from JLL provides the most comprehensive country comparisons in the world, allowing real estate investors, developers, and corporate occupiers to assess the difficulties and dangers of operating or investing in international markets. The GRETI, which was first published in 1999 and is now in its ninth edition, examines real estate performance assessment, data availability, governance, transaction procedures, and legal and regulatory frameworks in 109 markets throughout the world. In the study of 2020, **Romania** occupied the 35th position having an Overall Score of 2.71, Investment Performance 4.03, Market Fundamentals 2.78, Listed Vehicles 1.80, Regulatory Legal 2.18, Transaction processes 1.46 and Sustainability of 3.36. The best score was obtained by United Kingdom, United States and Australia.

30	South Korea	AP	2.57	3.28	2.26	2.25	1.90	2.43	3.45
31	Luxembourg	EUR	2.59	3.12	2.95	2.55	1.88	1.75	3.64
32	China - SH/BJ	AP	2.59	2.72	2.09	2.54	2.46	2.42	3.73
33	Thailand	AP	2.64	3.09	2.45	2.11	2.20	2.31	3.91
34	India	AP	2.69	3.55	2.35	1.92	2.63	1.92	3.18
35	Romania	EUR	2.71	4.03	2.78	1.80	2.18	1.46	3.36
36	UAE - Dubai	MENA	2.75	3.42	3.12	1.66	2.52	1.97	3.27
37	Israel	EUR	2.80	3.38	4.09	2.18	1.63	1.39	4.73
38	Russia	EUR	2.81	3.57	2.12	1.98	2.55	2.41	4.09
39	Mexico	AM	2.83	3.36	2.89	1.80	2.66	2.50	3.36
40	Indonesia	AP	2.86	3.19	2.11	2.42	2.62	2.72	4.45
41	Greece	EUR	2.86	3.37	3.26	2.20	2.51	2.20	3.36
42	Bulgaria	EUR	2.87	3.76	3.39	2.50	2.08	1.84	3.55

Figure 3: Part of the table covering Romania [JLL]

2.2 Tansaction Cost

Transactions are separated into two sorts for ease of understanding: transactions without history (data transactions) and transactions with history (money transactions). Data transactions are transactions from databases, sensors, and IoT networks that are independent of each other and may or may not be connected to previous transactions. For example, power consumption data given by a power sensor is independent of past readings and may be verified without them.

Financial transactions, on the other hand, are transactions involving token/asset transfers that need verification of prior transaction trails. Person A, for example, transfers 100 tokens to Person B. This transfer can only be validated by looking at Person A's prior transaction trail to see if he/she has enough tokens to complete it. Because the features of these two types of transactions are distinct, creating a system that secures both becomes more difficult. Designing a system to safeguard financial transactions, for example, may not be difficult because it entails tracking a transaction trail. However, when we choose to build it for a resource-constrained system (such as distant IoT devices), the level of complexity increases dramatically. Likewise, determining the legitimacy of data exchanges is difficult due to the lack of a transaction trail. Furthermore, when the source is a resource-constrained system, such as a distant IoT device, ensuring its authenticity is just as crucial as ensuring its validity.

The costs of buying or selling a product or service are known as transaction costs. Transaction costs indicate the time and effort required to bring a product or service to market, and they have given rise to entire enterprises dedicated to making transactions easier. In the financial sense, transaction costs include broker fees and spreads, which are the differences between the price the dealer paid for a security and the price the buyer pays.

The revenues that banks and brokers earn for their responsibilities are known as transaction costs to buyers and sellers. There are extra transaction expenses when buying or selling real estate, such as the agent's commission and closing costs, such as title search fees, appraisal fees, and government fees. Another type of transaction cost is the time and effort required to move items or commodities over long distances.

An economy gets more efficient as transaction costs fall, freeing up more capital and labor to create value. As the labor market adjusts to its new surroundings, a transformation of this magnitude is not without its challenges.

The real estate agent's fee in Romania is up to 6% of the transaction value, however the entire amount is shared equally between the two parties participating in the transaction. In other words, a 3% real estate agent's fee applies to both the buyer and the seller. All of these transaction fees are intended to provide the investor an idea of whether they can afford to buy real estate in Romania and what their financial safety level should be. Following the completion of the transaction, Romanian law establishes a separate self-standing tax payment system on properties and land.

Blockchain might be used to eliminate intermediaries from real estate transactions, lowering expenses. A decentralized network's transparency can aid in the reduction of real estate transaction costs. In addition to the savings obtained by removing intermediaries' professional fees and commissions, other expenditures associated with real estate include inspections, registration fees, loan fees, and taxes. Depending on the jurisdictional territory, these charges vary significantly. As platforms automate and integrate these procedures, they, like intermediaries, may be reduced or even eliminated from the equation. Despite the fact that worldwide real estate is worth hundreds of billions of dollars, it is dominated by the wealthy and large corporations. As a result of blockchain technology, which makes transactions more transparent, secure, and egalitarian, more people may be able to access the market. In the future, real estate transactions may become truly peer-to-peer, with blockchain-powered platforms doing the majority of the work [Con22].

2.3 Usage of Smart Contracts

Smart contracts are a very valuable feature that has emerged from the usage of blockchain technology in bitcoin and other applications. Smart contracts are already having an influence on many aspects of business and society — perhaps you've heard of NFTs — but they're especially well positioned to transform real estate. Before we look at how smart contracts will change the real estate industry, it's important to know what smart contracts are and what they do.

On decentralized networks, smart contracts are self-executing apps. Smart contracts' underlying automation eliminates the administrative cost involved with tracking transactions in an exchange with established rules and conditions. The blockchain, or decentralized network, verifies the transactions by comparing them to pre-set criteria. Smart contracts are a type of automation that digitizes company regulations and replicates them in the blockchain protocol (software) that oversees the exchange.

The blockchain approach has the potential to deliver various benefits to the real estate industry:

- Smart Contracts are self-executing automated contracts that have precise instructions specified in their code that are performed when certain criteria are met (similar to IFTTT logic).

- Tokenization: A token is a digital representation of an item, value, or function in the real world. The tokenization of real-world assets is one of the most fascinating applications of blockchain technology.

Although the usage of blockchain and smart contracts may assist to eliminate all intermediaries (brokers, banks, and attorneys), it will not eliminate local government restrictions. Furthermore, due to the massive amount of paperwork, intermediaries, and lack of transparency that you must go through, Real Estate transactions may be incredibly sluggish and take months. We will be able to speed up this procedure in a hypothetical scenario with transactions running through a blockchain network. It is possible to link the digital ownership of the property, documents, and contracts directly into the blockchain using smart-contracts. The owner is safe since the data can't be tampered with or changed once it's within the blockchain.

Another idea here, may be: Rather than owning a single property, numerous people might acquire tokens and co-own the structure.

- It is possible to divide property ownership.

- Micro-investors can buy a piece of real estate for a little fee.

Let's have a look at an example: A Mamaia seaside property would cost roughly \$600.000, which is out of reach for most people, including myself. Assume the owner is willing to tokenize the property and sell it on a public exchange in order to attract additional investors. The purchase orders were executed by five consumers, resulting in a total of \$120,000 in tokens. After completing a multi-signature smart contract on the blockchain network, they now jointly own the house. With a multi-signature smart contract, new investors may rest certain that all future choices will be made when a majority of the owners have agreed. It may sound unbelievable, but it is something that might be constructed to assist automate the process of getting started investing in real estate at a lesser cost than the usual method.

For example, in Australia, there is currently a website called BrickX that allows you to acquire fractionalized real estate shares for as little as \$100. However, blockchain technology has the potential to take this concept much farther. As can be seen, tokenization has the power to enhance liquidity. It helps you to diversify your portfolio and maybe reduce your risk exposure. Instead of investing all of your money in one property, you may use the same cash to purchase fractions of many properties and earn a dividend if the property is rented out or a profit if you sell your Tokens. On the other side, fractional ownership reduces the barriers to entry into the real estate market. To buy a huge house, you won't need to save or take out a large loan; instead, you may buy a part of the property you wish to invest in.

3 Blockchain

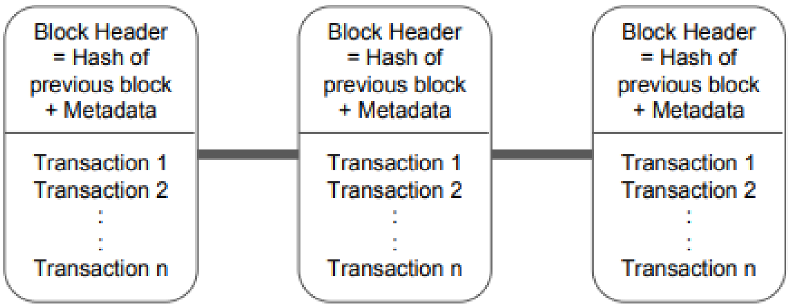


Figure 4: A blockchain structure

Despite its technical description, blockchain should be viewed as a new way of thinking. After the internet, it is regarded as the most recent revolutionary and disruptive technology. The internet offered a new degree of communication to its predecessor technology, the Personal Computer, and it adds a new level of confidence to the internet without the need for a third trusted party's participation. Blockchain is a public ledger utilized by the Bitcoin network, according to its technical definition.

Bitcoin makes use of a 1976 innovation called public key cryptography, as well as an internet-based idea called peer-to-peer communication, as well as blockchain to improve its network and establish an automatic agreement. Peer-to-peer communication is not new however; BitTorrent, for example, uses it to service its 45 million users. This new paradigm may be used to a variety of situations. Decentralized payments and exchanges, asset invocation and transfer, smart contract creation and execution, and peer-to-peer value transactions are just a few of this technology's capabilities.

The definition of the internet might help you better comprehend the reach of this technology and how important this ledger can be. The Internet is an interconnected network that employs transport protocols to create communication between each of the network's nodes. Participants can send data through these connections to obtain the desired level of communication.

In the early 1990s, E-mail was the sole widely used internet application. Having said that, it's easy to envision how far-fetched today's internet applications would have seemed in the 1990s. However, IBM executives believed that there was no need for more than four mainframe computers ("I think there is a world market for maybe five computers." - Thomas Watson, president of IBM, 1943) [Wil17] in the globe because existing internet users, who will almost certainly have access to a computer by July 2018, are anticipated to number more than four billion.

In simple words, a blockchain is a collection of blocks (each carrying data) that are connected together using cryptographic processes to build a strong chain. This allows it to record transactions in a safe and verifiable manner without the use of a third party. In most circumstances, the preceding block's hash is the only one that is included in the current block's construction. The notion of blockchain has been around for over three decades.

Stuart Haber and W. Scott Stornetta revealed the first application of the blockchain concept in 1991 in their paper "How to Time-Stamp a Digital Document" [SH91]. However, Bitcoin, the first cryptocurrency built on blockchain, propelled the technology to popularity in 2008. Since then, the economics of blockchain-cryptocurrencies have evolved, with a total market capitalization of almost 2 trillion - $1,832,696,539,775 [coi12] (28 April 2022).

A block on the blockchain, in its most basic form, comprises data separated into several discrete units known as transactions, as well as a hash of the preceding block. Figure 4 illustrates the structure. Blockchain is built on Distributed Ledger Technology, and it achieves immutability by keeping ledger copies securely on all participating nodes. Different consensus algorithms (consensus based on Proof of Work (PoW), Proof of Stake (PoS), Proof of History (PoH), and others) are used to achieve coherency. The

Peer to Peer (P2P) network is formed by the participating nodes, and a communication protocol is implemented among them to carry out information dissemination.

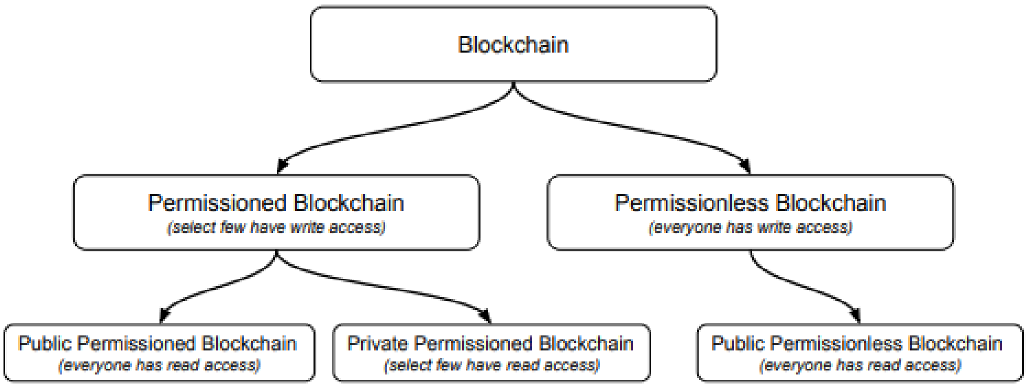


Figure 5: Classification on permission

According to numerous factors such as permissions, application domain, protocols, and so on, blockchain may be classified into a wide range of categories. It may be divided into two groups based on permissions: permissioned and non-permissioned. Prerequisite permissions are required to connect/read/write on a permissioned blockchain, but no explicit rights are required on a non-permissioned blockchain. (Figure 5)

The two primary types of blockchains based on application areas are Transaction Optimized Blockchains and Code Optimized Blockchains. Transaction optimized blockchains are largely used for the transfer of assets and to some extent for data storage, whereas code optimized blockchains are mostly used for the execution of code on the blockchain. The overhead of code optimized blockchain is frequently higher than transaction optimized blockchain since there are more virtual machines functioning on each participating node for the execution of code, and there are also more messages for sharing the current state of variables. [VD19]

3.1 History of payment systems

A payment happens when one party, the payer, transfers an asset to another party, the payee, in order to pay off a debt that the payer has incurred. Alternatively, a payment might be the payer instructing a third party to make such a transfer. While a payment can be made with any asset in theory, practically all contemporary payments are made with debt claims held by either a central bank ('outside money' in the form of both currency and deposits) or private banks ('inside money', which is almost exclusively in the form of deposits).

A payment system, on the other hand, is made up of a set of technologies, regulations, and contracts that allow for payments to be made and specify when they are deemed resolved. Examples include currency, checks, credit and debit cards, electronic financial transfers, internet banking, and other payment methods. The proper operation of such systems is important to the development of developed economies. On the one hand, payment systems encourage the use of credit and consequently economic activity in general by providing debtors with low-cost and reliable ways to settle their obligations. Insecure and inefficient payment methods, on the other hand, may obstruct the effective flow of payments between people and economic entities.

However, while money has been used as a means of payment for a long time, payments between economic agents were mostly restricted to basic bilateral connections - one agent would create a thing, and a consumer would pay for it with some kind of money, either commodity or fiat. It took the creation of banks to create the circumstances for the more sophisticated development of payment economics.

Modern banks arose from a variety of beginning places. Bankers in the medieval Middle East, for example, not only exchanged money and granted loans, but also used a variety of payment methods on a daily basis. Even though merchants and bankers in Europe were aware of these procedures when trading in and with Muslim countries, there is no concrete proof that Middle Eastern payment methods were immediately adopted [Ash73].

The rise of cryptocurrencies like Bitcoin and Ethereum has reignited interest in privately produced money, but the monetary literature on the subject is still in its infancy. Fernández-Villaverde and Sanches create an interesting model of competition among privately produced fiat currencies from which they extract three primary conclusions [FVS16]. They are among the few who have tackled this topic. For starters, price stability may be achieved in the presence of competing private money. Second, even when issued by profit-maximizing, long-lived entrepreneurs who care about the future worth of their currencies, private monies are prone to self-fulfilling inflationary episodes. Third, a totally private monetary system does not offer the most money for the most people. That is, the market fails to give the appropriate quantity of money while providing the appropriate number of other products and services.

David Chaum established the concept of digital payments and digital currencies for the first time in history in the 1980s. Some institutions sought to market Chaum's proposal by introducing E-gold and E-money [J.16]. Despite all attempts, the commercialization of cryptocurrencies failed due to a number of factors, including a lack of centralized network structure, centric-based networks, and regulatory benchmark compliance. A system that was more secure, decentralized, and transparent was required.

When Satoshi Nakamoto created bitcoin in 2008, it was the first time blockchain was mentioned [Nak08]. Nakamoto advocated completely digitalized currencies that work on a decentralized system, eliminating the need for a trusted third party to address the double-spending problem. Despite the technology's early debut this millennium, nothing has transpired with it, but in recent years (particularly 2015 and beyond), blockchain has become a hot subject. For the usage of digital payments, contracts, and other services, a more secure, decentralized, and transparent system is required, much as it was in the 1980s.

In 2015, Goldman Sachs, Barclays, JP Morgan, Royal Bank of Scotland, Credit Suisse, and a few more banks teamed together with R3, a financial technology company. The only goal is to provide a framework for implementing blockchain technology in the financial industry. [Cro15]

3.2 Cryptography

The study of secure communications systems that enable only the sender and intended recipient of a message to read its contents is known as cryptography. The word "kryptos" comes from the Greek word "kryptos," which meaning "hidden." It's closely linked to encryption, which is the process of scrambling plain text into ciphertext and then back again when it's received. In addition, cryptography includes techniques such as microdots and merging to obfuscate information in photographs. Ancient Egyptians were known to use similar tactics in complex hieroglyphics, while Roman Emperor Julius Caesar is credited with inventing one of the earliest modern ciphers.

The most common use of cryptography when transmitting electronic data is to encrypt and decode email and other plain-text messages. The most basic method is the symmetric or "secret key" technique. The secret key is used to encrypt the data, and the encoded message and secret key are then sent to the recipient for decoding. What exactly is the problem? If the message is intercepted, a third party has all they need to decode and read it. To solve this difficulty, cryptologists devised the asymmetric or "public key" approach. In this example, each user has two keys: one public and one private. Only the recipient's private key can decode the message when it arrives, therefore theft is useless without the associated private key.

Cryptography is critical in today's internet environment, with the vast volume of security-sensitive information being transported around the globe over the internet.

Cryptography's main objective is to establish secure and private communication methods. Intruders or adversaries may listen in and even manipulate the communication channel if encryption was not used. With cryptography, a user may communicate information to another user without the information being intercepted by an unknown third party. Cryptography is used not just to prevent intruders and adversaries from intercepting information, but also to ensure that the information is not tampered with and that it is delivered from the correct user.

Three forms of cryptography are employed in blockchain technology:

- Public key cryptography for transactions

- Hash functions to safeguard data inside the blockchain

- Symmetric key cryptography protects the private key within the user's wallet

3.3 Public key cryptography

Public key cryptography is a security mechanism that assures the security of data sent in a blockchain network transaction. In a point-to-point network such as blockchain, security is critical. Because nodes in such a network do not know and trust each other personally. There is a requirement for a strong security system to be in place. One that ensures the security of the data they send or receive without having to worry about security breaches. This also eliminates the necessity for all nodes to know and trust one another on a personal level.

The usage of a pair of keys in public key cryptography is an asymmetric kind of encryption (public key and private key). It makes use of them to encrypt/decrypt data and verify users. The public-key cryptography procedure assures two things. i.e,

1. At the sender's end, the information is encrypted using the public key (of the receiver). This ensures that no one outside the network can see or comprehend the encrypted data flowing in and out. Using its own private key, only the intended receiver may decode and read the message.

2. Using the sender's private key to sign the message or content for verification. This verifies the sender's identity and confirms that he is a valid node in the blockchain network. The sender's public key is used by the recipient to verify this. Digital signatures are used to verify the identity of users in a network.

We utilize a pair of keys: a public key and a private key. The Elliptic Curve cryptography technique is used to produce both of these keys. It first generates a private key, then uses the Elliptic Curve Algorithm to generate a public key from the private key. As a result, the private and public keys are cryptographically and mathematically connected. One thing to keep in mind is that the process of producing a public key from a private key is irreversible. That is, we can get the appropriate public key from its private key, but not the other way around. The procedure is constructed in such a manner that brute-forcing the private key needs a lot of computer power and time, which is nearly impossible.

The digital wallets (software or hardware) essentially store the private key as its security is very important. The usual format for storing the key is a wallet import format which has a 51 character long key. This length may vary depending upon the storage formats.

Let's use a hypothetical case to explain how public-key cryptography works. Andrei wants to use the blockchain network to deliver a message to Radu. This information exchange between two nodes on the blockchain is referred to as a "transaction."

Step 1: Andrei will encrypt the message he wishes to communicate with Radu using his public key. The message will be converted into an unreadable format as a result of this.

Step 2: Andrei will now take the hashed message and use his private key to sign it. This is referred to as "digitally signing" the deal (digital signature).

Step 3: Andrei is now prepared to deliver this message to Radu over the blockchain network. However, Andrei must first get the transaction confirmed by the whole blockchain network. Every node on the network will validate Andrei's digital signature and pass the transaction using Radu's public key.

Step 4: Radu will get the message after successful verification, but it will be in an encrypted form known as ciphertext. First and foremost, Radu will use his public key to authenticate Andrei's digital signature.

Step 5: Radu will then use her private key to decipher the ciphertext. The message will be converted to a readable format as a result of this action.

Step 6: The transaction is completed successfully. It is also permanently stored on a new block on the blockchain. No one can doubt that Andrei and Radu participated in a transaction.

3.4 Consensus Protocol

We use the term "consensus" to refer to a universal agreement. Consider a group of individuals who are going to see a movie. A consensus is reached if there is no dispute about a proposed film option. In the worst-case scenario, the gang will break up. In the case of blockchain, the process is formalized, and obtaining consensus implies that at least 51% of the network's nodes agree on the network's next global state.

Consensus algorithms (also known as consensus protocols or consensus mechanisms) allow decentralized systems (computer networks) to function together safely.

For decades, these methods have been used to reach consensus among database nodes, application servers, and other corporate infrastructure components. In recent years, new consensus algorithms have been developed to allow cryptoeconomic systems like Ethereum to agree on the network's state. A consensus mechanism in a cryptoeconomic system also contributes in the avoidance of certain sorts of economic attacks. An attacker can hypothetically risk consensus by controlling 51 percent of the network. To prevent this "51 percent attack," consensus safeguards have been put in place. To solve this security issue in various ways, numerous techniques have been created. A consensus mechanism allows the blockchain network to achieve dependability and create trust amongst nodes while maintaining environmental security. This is why it is an important aspect of every dApp project in the distributed ledger ecosystem. These algorithms operate on the ground of different objectives, a few of which we will be covering in the following subchapters.

Objectives:

1. Unified Agreement

The achievement of unified agreement is one of the primary goals of consensus processes. In contrast to centralized systems, where confidence in authority is required, users in a decentralized system can work without creating trust in one another. The protocols built into the Distributed blockchain network ensure that the data used in the process is correct and up-to-date, as well as the status of the public ledger.

2. Align Economic Incentive

When it comes to creating a trustless system that controls itself, it's critical to align the interests of network participants. In this situation, a consensus blockchain protocol rewards good behavior while punishing bad actors. This also guarantees that economic incentives are regulated.

3. Fair Equitable

Consensus techniques allow anybody to join the network and utilize the same fundamentals. In this sense, the blockchain system's open-source and decentralized properties are justified.

4. Prevent Double Spending

Consensus mechanisms function on the basis of algorithms that ensure that only verified and legitimate transactions are published in the public transparent ledger. This eliminates the problem of double-spending, which occurs when a digital currency is spent twice.

5. Fault Tolerant

Another advantage of the Consensus approach is that it makes the blockchain fault-tolerant, consistent, and dependable. That is, even in the face of failures and threats, the regulated system would continue to function. There are now a variety of consensus algorithms in use in the ecosystem, with many more on the way. As a result, every Blockchain development business and aspiring entrepreneur must be aware with the characteristics that characterize a good consensus protocol, as well as the consequences of choosing a bad one.

3.4.1 Proof-of-Work

Proof-of-Work is the initial consensus process in Blockchain networks, in which users exchange digital tokens, verify transactions or even add new blocks to the chain. To be paid, all miners or validators participate in this method by carefully validating and confirming transactions on the network. The distributed ledger collects all validated transactions in the network and organizes them into blocks. Mining is the term for this procedure. Proof of work is a mechanism that protects against cyber threats such as distributed denial-of-service (DDoS) attacks, which aim to deplete computer resources by sending repeated fraudulent requests. [HS18]

To find digital coins, the miner or validator must do difficult mathematical calculations. The correctly confirmed transactions are subsequently recorded in the next block, forming a new block group in the blockchain, a public distributed ledger. The purpose of mining is to check the authenticity of a transaction and to produce new cryptocurrency, which is mined by the awarded validators for their previous labor. If the miner completes the job first, they will be awarded with new bitcoin, which will encourage more miners. Furthermore, the mining process increases network processing power and computation, causing the mining process for a coin to grow, making it more difficult and expensive for a single miner.

During the transaction creation process, the following events occur:

1) A block contains all transactions

2) Each block's transactions are validated by miners

3) Miners / validators resolve mathematical puzzle called proof-of-work

4) The miner/validator who settles the first transaction in each block is awarded as the first winner

5) Finally, verified transactions are added to the public blockchain.

This mathematical computation is asymmetric and the work required is complex. Mining follows inverse hashing, where it finds number (nonce) so that the hash algorithm of block information is to be more lesser than the provided threshold (complexity). The threshold marks the effort, calculations, and energy needed to mine a new block. This also increases the miner's mining efficiency. A new block is created every 10 minutes during this update, which happens approximately every 14 days. Miners put in a lot of effort and are paid for making the network's node and blockchain more secure. Proof-of-work is a more complicated computing technique that prevents old blocks in blockchain from being modified.

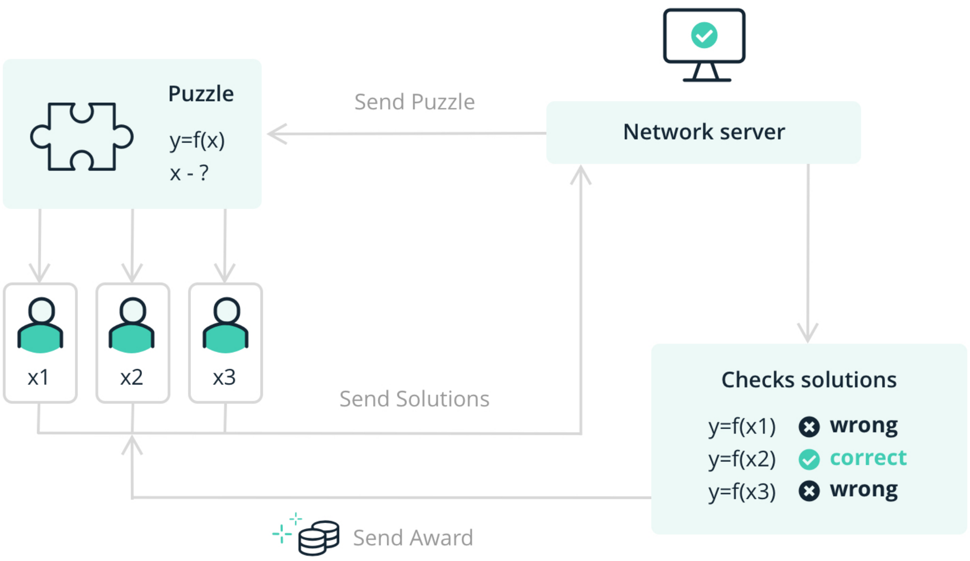


Figure 6: Proof of Work [SAS19]

3.4.2 Proof-of-Stake

Proof-of-stake (PoS) is a consensus technique that has the same goal as proof-of-work but differs in the process of validating transactions in a distributed network. Proof-of-stake is based on a monetary value called stake. A stake is a sum of money that is locked up for a specific length of time. Unlike proof-of-work, there is no monetary incentive for verifying and confirming transactions within a block; instead, miners get transaction fees for completing the process. PoS is stake-based, focusing on the quantity of cryptocurrencies on the blockchain to produce new blocks rather than wasting a lot of resources, energy, or processing power like PoW. Proof-of- Stake is related to the size of the network and the number of persons that stake the digital currency. There will be less awards if a large number of individuals stake the currency. Furthermore, if users hold more cryptocurrency for a longer length of time, they will be rewarded with higher transaction fees; however, the process should be spread around the network to avoid one individual from controlling the coin. This concept operates in the same way as a bank fixed deposit, where the consumer gets greater interest for storing a large sum of money for a longer period of time.

In PoS, a creator is chosen based on their wealth, which is the quantity of coins staked. The forger is the individual who validates the transaction and creates a new block. To generate a new block, the forger stakes their money and validates the transactions to add a new block. If the validator verifies any fraud transaction, they may lose their share and authorization to proceed. It is now necessary to choose the forger who will forge the next block. The right method for choosing a forger is as follows:

1) Randomized Selection- The person with the lowest hash value and the most stake will be able to choose the next block.

2) Coin Age-Based Selection- The forger is chosen based on the coin's age.

Figure 7: Proof of Work

3.4.3 Proof-of-History

The Solana Network's main invention is Proof of History, which is exactly what it sounds like: proof of historical occurrences. Proof of History establishes a historical record that establishes that an event took place at a given point in time. Unlike other blockchains, which require validators to communicate with one another in order to agree that time has passed, each Solana validator keeps track of time by encoding it in a simple SHA-256, sequential-hashing verifiable delay function (VDF). This differs from the current standard of blockchain infrastructure, which relies on a sequential production of blocks that are hindered by waiting for confirmation across the network before moving forward. Proof of History presents a fundamental move forward in the structure of blockchain networks in regards to speed and capacity.

Proof of History works like this: The Solana data structure is a message chaining system. This gives a cryptographic evidence of each message's relative order and time in the historical record. As the data structure is finally delivered and reassembled, the network may disregard local clocks and progressively accommodate all potential network delays. This is how Solana is able to push the boundaries of confirmation times, allowing the network to give an experience comparable to that of a centralized system while maintaining security and decentralization. [Yak19]

Messages do not have to arrive at a validator in a certain amount of time. Every validator eventually receives the ledger, and because the messages are included in the ledger, PoH gives a cryptographic assurance that the messages were produced when they claimed. This attribute enables us to improve the network across a variety of factors, most notably block time, which is a critical component of blockchain infrastructure in terms of speed and efficiency. PoH allows Solana to optimize for block propagation (log200(n)), throughput (50K-80K TPS), and ledger storage (petabytes) on the network in addition to Block Time.

As a result of this capability, the network is never delayed and can continue to create at lightning rates despite block producer differences. Proof of History is a strong concept that allows blockchain technology to achieve network speeds never seen before. Solana is the first web-scale blockchain with transactional capacity comparable to the present internet, thanks to features like Tower BFT, Turbine, and Replicator nodes.

3.5 Usage of Smart Contracts

Smart contracts are programs that execute when specific circumstances are satisfied and are stored on a blockchain. They're often used to automate the execution of a contract so that all parties may be confidence in the conclusion immediately away, without the need for any middlemen or wasted time. They can also automate a workflow by initiating the next phase whenever certain conditions are met.

Simple "if/when...then..." lines are inserted into code on a blockchain to make smart contracts operate. The actions are carried out by a network of computers after the predefined conditions are met and approved. Sending notices, dispersing payments to the appropriate persons, or issuing a ticket are examples of these activities. The blockchain is updated after the transaction is completed. This implies that the transaction can't be changed, and the results are only available to those who have been given permission to see them. A developer can then write the smart contract, however businesses that use blockchain are increasingly giving templates, web interfaces, and other online tools to make smart contract creation easier. [Rob]

Once a condition is satisfied, the contract is instantly executed. There is no paperwork to deal with, and no time wasted fixing errors that might occur when filling out papers manually, because smart contracts are digital and automated. There's no need to worry about information being tampered with for personal gain because there's no third party engaged and encrypted transaction logs are exchanged among participants. Blockchain transaction records are particularly difficult to attack since they are encrypted. For the reason that each entry on a distributed ledger is connected to the entries before and after it, hackers would have to alter the entire chain in order to change a single record. Smart contracts reduce the need for middlemen to manage transactions, as well as the associated time and costs.

On the Ethereum blockchain, the ERC-721 token standard is used. A more common term for these assets is non-fungible tokens, an asset class that increased in popularity in late 2020 and early 2021. Non-fungible tokens (or NFTs) are tokens with unique characteristics that set them apart from other tokens. [DEV22]

A $10 note is an example of something that is fungible. You don't have to get the exact same banknote back if you lend one to a buddy because they're all identical.

A non-fungible item is something like an airline ticket or a trade card. Although two plane tickets may appear identical, one may offer an economy flight to Cluj-Napoca and the other a first-class flight to Dubai. As a result, they are unable to be swapped like-for-like.

ERC-721 tokens enable this notion to be implemented on the blockchain, ensuring that unique details about an asset can be preserved. NFTs can be used to create a digital depiction of a one-of-a-kind artwork with easy-to-prove ownership via blockchain records. This may aid in the fight against counterfeiting. The Ethereum community is convinced that ERC-721 will have a wide range of applications, far beyond the collecting CryptoKitties that made this asset class popular. A number of competing blockchains (such Binance Smart Chain) have also produced token standards that are similar to ERC-721.

4 The proposed work

The act of producing a digital asset in the form of a token on a blockchain-based system utilizing distributed ledger technology is known as real estate tokenization. Whoever buys such token will possess a piece of the property in a fractional way. Blockchain technology aids in the decentralization of the whole crowdfunding and tokenization process. It removes the need for middlemen like as brokers, banks, and attorneys. It handles a variety of tasks, including listing properties, accepting payments, and preparing legal documents. It assures data sharing transparency by using an immutable distributed ledger. This eliminates the possibility of deception. It improves the safety and fairness of property investment.

The solution for the tokenization of real estate industry consists in a software application which helps the users make transactions with houses or apartments on the blockchain. The platform is developed using Solidity 0.8.4 and ReactJS 17.0.2 with the corresponding NodeJS libraries like ethers.js, axios, swiper and others.

One of the first functionalities of the platform is the sign up. Sign up referrs to the creation of an online account using an e-mail address or Google account. The users will be stored on Firebase Authentication and their profile on Firebase Firestore which is a cloud-hosted, NoSQL database. Here are the sequence diagrams for this functionality:

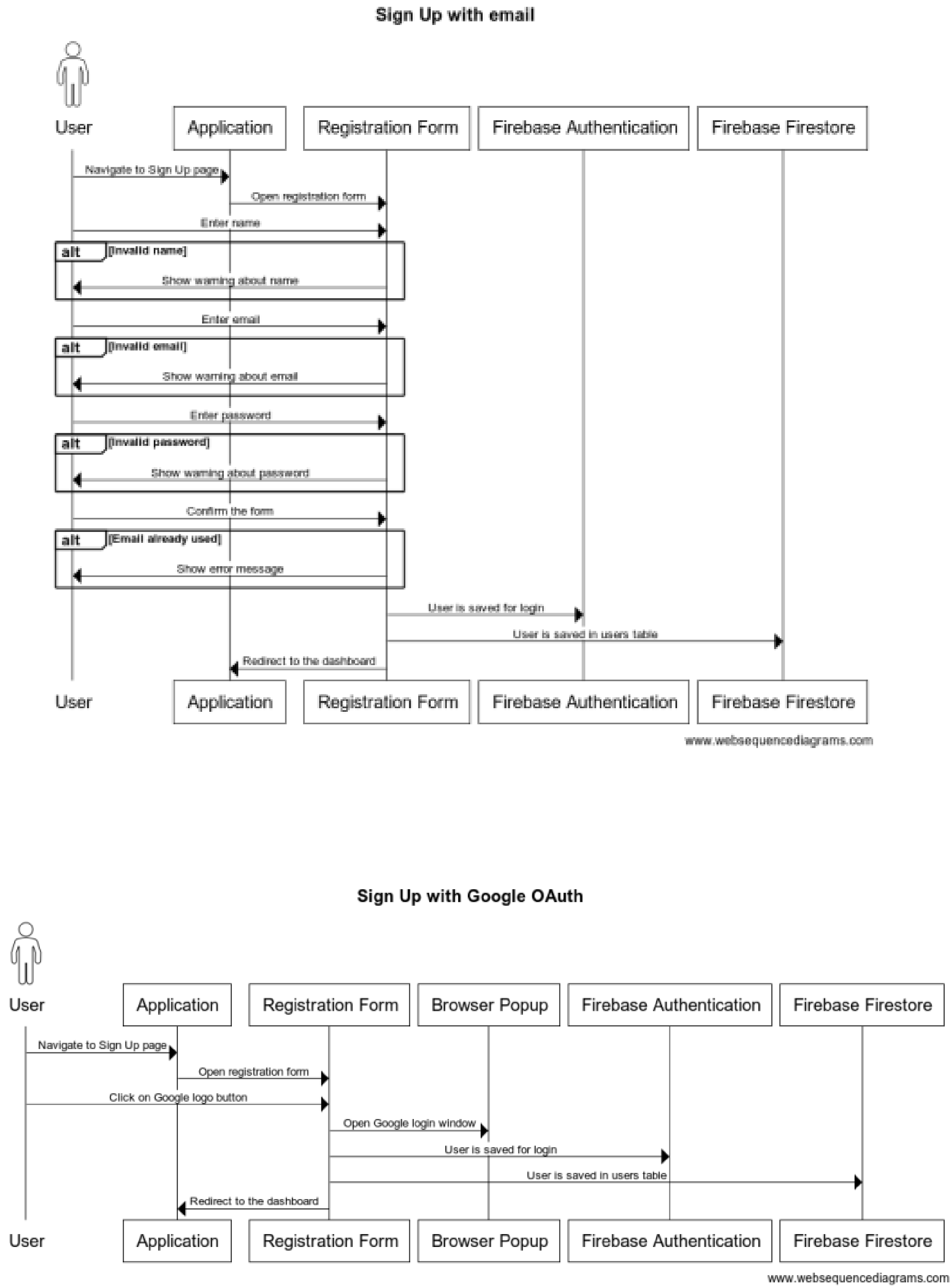


Figure 8: Sequence diagram for Sign Up

After a user creates an account on the platform, he can login afterwards, either with the default email address or with his Google account. After the completion of the form, a request will me made to the Firebase servers to check if those are correct. If the credentials are good, it will be redirected to dashboard page, otherwise there will be an error message shown. There is the sequence diagram for this functionality:

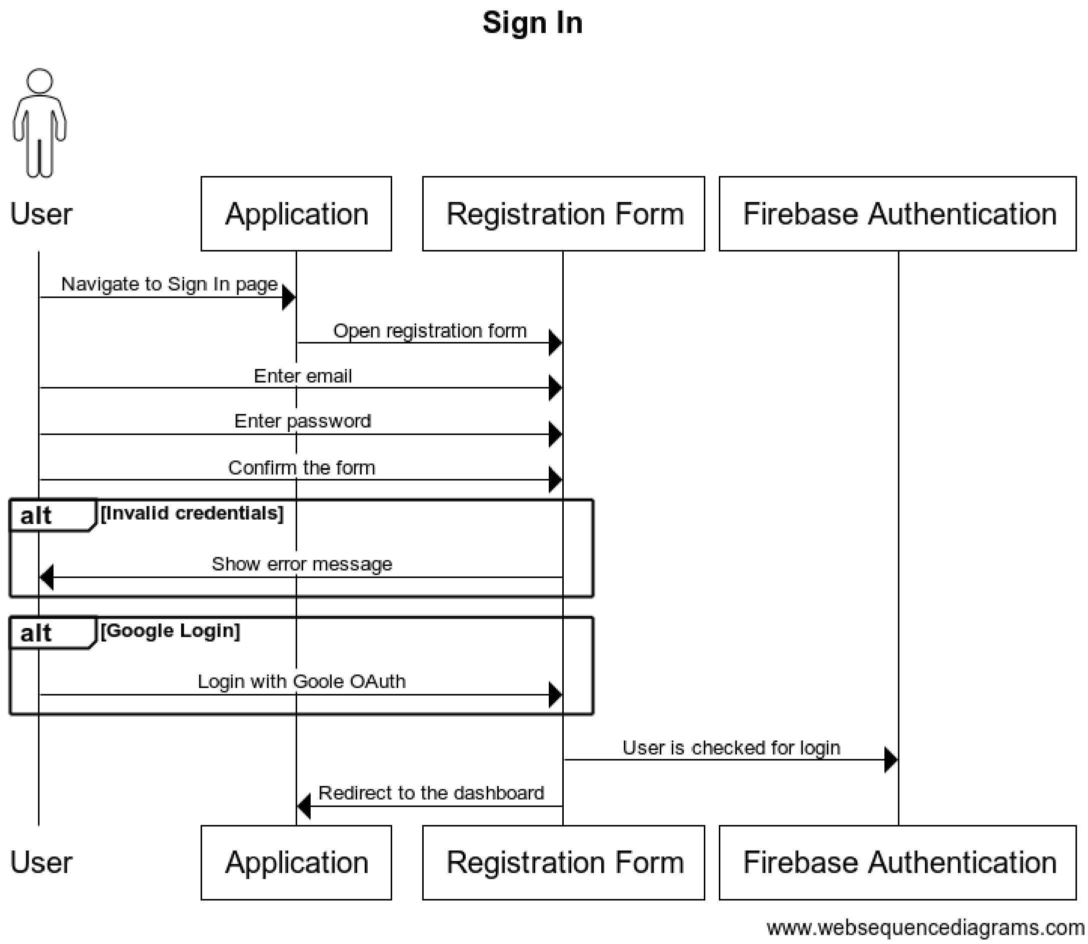


Figure 9: Sequence diagram for Login

A very important functionality of the platform is the addition of listings, which then other users can buy using Ether. It consists of going to the Profile Page and clicking on the "New Listing" button, then the form is opened. The user has to input if the listing is a house or an apartment, the name, the number of bedrooms and bathrooms, check if it has a parking spot, check it is furnished, input the address, regular price and the discounted price if it has an offer. Then he has to add images and most important, the Ethereum address where the payment can be done. After a confirmation, this listing will be added to Firestore and other users can view it on the platform.

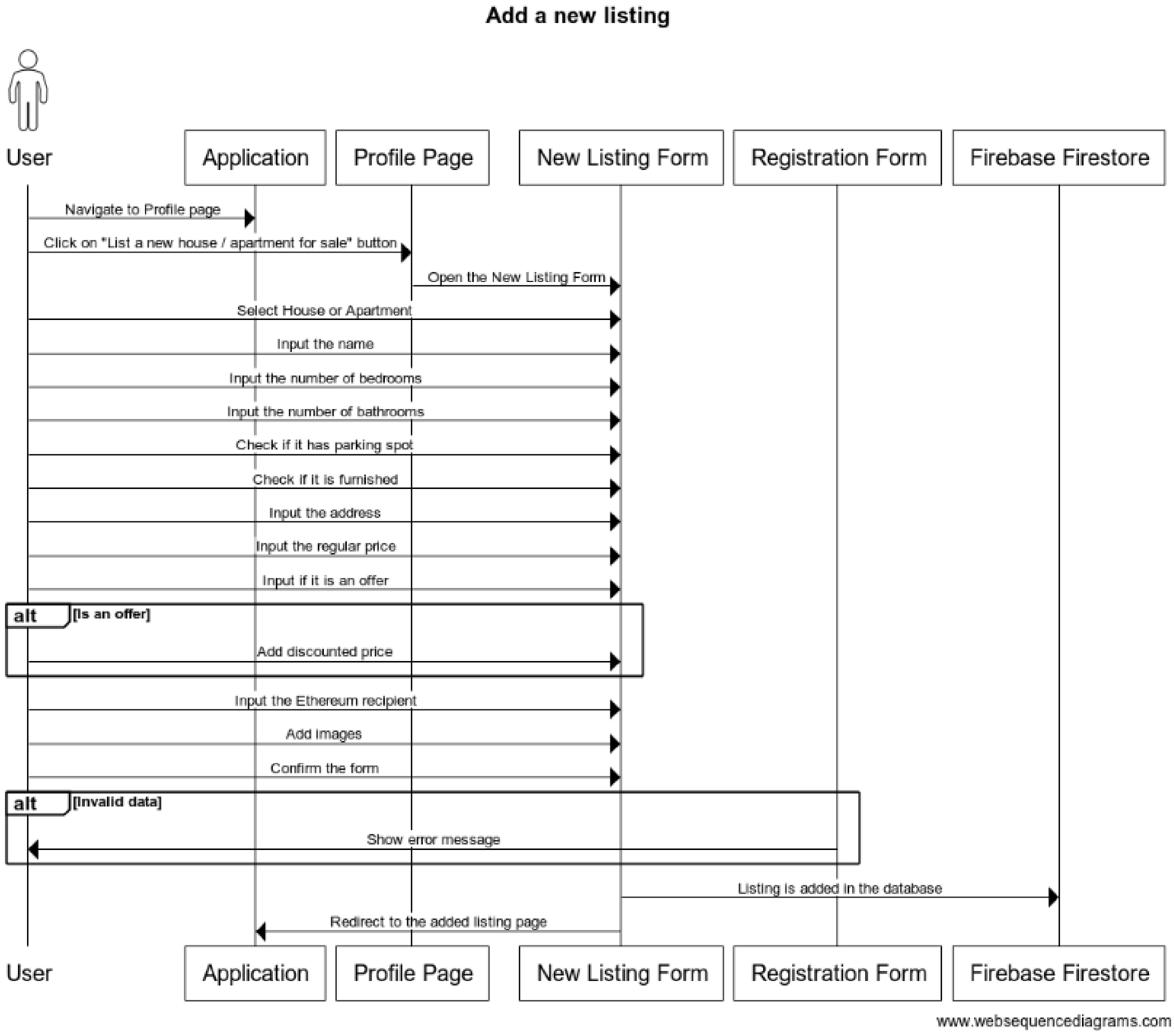


Figure 10: Sequence diagram for adding a listing

In order to navigate to this page, the user must be logged in, otherwhise he is redirected to the Login Page. According to the given location, the application is using in the background a Google Maps API and after the form is completed, it will find the coordinates of the given address, so that a point will be shown on the saved listing's map. An Ethereum account has an Ethereum address, like an inbox has an email address, so the user should input a valid one. If there will be an error on adding a new listing, an error message will be shown in the top right corner of the screen, like for example if we add too many photos (more than six).

Now, the most important functionality which makes this platform relevant to a solution for real estate transactions using blockchain technology is the buying functionality.

Here is its sequence diagram which will be explained afterwards:

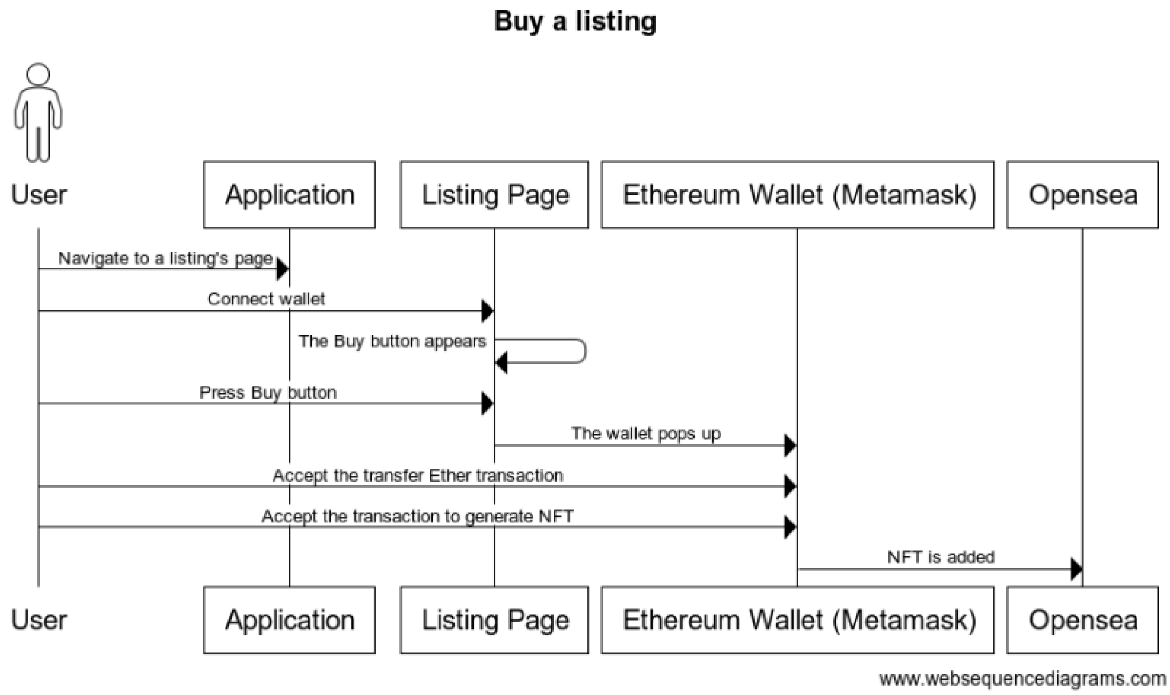


Figure 11: Buy a listing with Ether

In order to purchase a house or an apartment from the platform, the user must have an Ethereum wallet, most popular one being Metamask. Only if the user is logged in on the platform, he will see after the listing's photos and details a button with the text "Connect wallet". Pressing this, the Metamask window will pop up and the user should connect its wallet to the webpage. If the session is not saved in the Metamask, he will also need to input his password. When the wallet is successfully connected, a new button will appear with the text "Buy with Ethereum". Going forward, the Metamask popup will appear again and in order to buy the given listing, the user must accept two transactions: first one is to transfer ether to the listing's address and the second is to generate an NFT. If this phase went successfully, the user will be able to see the property as a certificate on Opensea, a marketplace comparable to eBay, Etsy, and Amazon where all of the listed products are unique digital treasures in the form of NFTs that users may buy, sell, and mint [VAR22]. The platform is a decentralized peer-to-peer exchange that allows users to conduct trustless direct transactions with one another.

4.1 Ethereum

Ethereum is the world's first general blockchain platform, allowing users to quickly design and deploy decentralized and trustless applications. It has opened up great possibilities in the financial industry. In 2015, Ethereum was introduced as a Bitcoin hard fork. It's the second cryptocurrency created by Vitalik Buterin, a Russian-Canadian programmer and writer who is also a youthful prodigy. Vitalik, who previously worked on Bitcoin, was dissatisfied with the Bitcoin process and created Ethereum, an upgraded version of the blockchain architecture. It's like comparing apples and oranges when it comes to Bitcoin and Ethereum. Bitcoin and Ethereum were both brought to the market with different goals in mind. The main objective of Bitcoin was to establish an alternative digital currency in the market and, as a result, to establish a totally secure and transparent payment and transaction system. Ethereum, on the other hand, was created as a platform for facilitating peer-to-peer contracts and applications using its own native currency, ether. The major goal of ether is to make Ethereum's functionality easier to understand and monetize, allowing developers to create and run distributed applications (called Dapps). Ethereum also presented a groundbreaking new concept known as a smart contract, which is a "Turing complete" programming language. [Moh18]

Ethereum is a Turing complete blockchain platform in the sense that it provides a basis for programming languages that may be used to create contracts that can solve any sensible computational problem. The Ethereum Virtual Computer (EVM), a consensus-based virtual machine that decodes generated contracts into bytecodes and executes them on Ethereum network nodes, is in charge of Ethereum. It also employs algorithms to guard against denial-of-service assaults, which are common in bitcoin marketplaces.

In Ethereum there are three languages to write smart contracts with:

- Solidity

- LLL

- Vyper

Solidity was used for this real estate solution. We have a smart contract developed with Remix Ethereum IDE which is explained step by step afterwards:

```
pragma solidity ^0.8.4;

    import "@openzeppelin/contracts/token/ERC721/extensions/ERC721Enumerable.sol";
    import "@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol";
    import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
    import "@openzeppelin/contracts/utils/math/SafeMath.sol";

    contract RealEstateMinter is ERC721, ERC721Enumerable, ERC721URIStorage {

        using SafeMath for uint256;

        constructor() ERC721("RealEstateMinter", "REM") {}

        function mint(string memory _uri) public payable {
            uint256 mintIndex = totalSupply();
            _safeMint(msg.sender, mintIndex);
            _setTokenURI(mintIndex, _uri);
        }

        function sendViaCall(address payable _to) public payable {
            (bool sent, bytes memory data) = _to.call{value: msg.value}("");
            require(sent, "Failed to make transfer");
        }

        function tokenURI(uint256 tokenId) public view override(ERC721, ERC721URIStorage) returns (string memory) {
            return super.tokenURI(tokenId);
        }

        function supportsInterface(bytes4 interfaceId) public view override(ERC721, ERC721Enumerable) returns (bool) {
            return super.supportsInterface(interfaceId);
        }

        function _beforeTokenTransfer(address from, address to, uint256 tokenId) internal override(ERC721, ERC721Enumerable) {
            super._beforeTokenTransfer(from, to, tokenId);
        }

        function _burn(uint256 tokenId) internal override(ERC721, ERC721URIStorage) {
            super._burn(tokenId);
        }
    }
```

Figure 12: The smart contract written in Solidity

To develop the smart contract, we first import OpenZeppelin files. These files include classes to which our contract can be extended. Next, we're adding ERC721, the main OpenZeppelin file (ERC721 is the token type), ERC721Enumerable so we can keep track of the amount of tokens produced and their IDs, and ERC721URIStorage so we can store metadata URLs with NFTs when they're minted. This is so that solutions like OpenSea can use the information to extract the image, name, and description. The functions _beforeTokenTransfer, _burn, tokenURI, and supportsInterface are also overridden to their parent class functions. If you don't, the Solidity compiler will produce an error because it won't know what to do with the redundant functions in the parent classes.

The constructor() ERC721("RealEstateMinter", "REM") is called when the smart contract is deployed (in this case, Rinkeby Network was used). Following that, we'll create a mint function to do the NFT minting procedure. So that we can save the metadata, we'll give in the metadata URL as uri in the argument. Finally, we need to know how many tokens there are so that we can acquire the current token ID and allocate it to a new NFT. To mint the NFT, we use the _safeMint function with the arguments msg.sender (which specifies that the NFT should go into the wallet from whence the request was submitted) and _uri. After that, we create a token URI for the NFT. The function sendViaCall is used to transfer ether from the user's wallet to the listing's wallet.

The NFT data is called on an intermediary called Pinata.cloud which is a pinning service that allows users to host files on the IPFS network.

IPFS objects are used to hold all of the files in the system. Each object has a maximum storage capacity of 256 KBs. Each object can store links to other IPFS objects in addition to the 256 KBs of data. However, as you may have noticed, when it comes to a single object, space is restricted. At first glance, it appears that the system will have trouble storing files that are greater than the limit. However, this is not the case because the IPFS has a solution. An image can be used as an example of a file that is larger than 256 KB in size. The InterPlanetary File System splits and divides the file into multiple separate objects that do not exceed the 256 KB limit in order for it to be stored in the system. When the file is split, the system creates a new empty object that links to all of the image's data objects. This system is incredibly simple, yet it has the potential to be very powerful if used correctly.

Along with this decentralized storage system, IPFS has one key feature in common with a blockchain. This characteristic refers to the fact that once something has been saved in the system, it cannot be modified.

4.2 React

React is a JavaScript library for designing user interfaces with UI components that is open-source and free. It is supported by Meta (formerly Facebook) and a community of individual developers and companies. React may be used as a basis for single-page or mobile apps thanks to frameworks like Next.js. React, on the other hand, is entirely concerned with state management and displaying that information to the Document Object Model, necessitating the use of other frameworks for routing and client-side functionality.

In order to create a nice user experience, the next libraries were used to get a better user experience and most important, to implement out blockchain solution: Material UI (an open-source React component library that implements Google's Material Design; it includes a comprehensive collection of prebuilt components that are ready for use in production right out of the box), axios, ethers (for communication with the smart contract), swiper (for the sliders).

The navbar was made using Material UI and the slider in center with pictures is made using Swiper. When clicking on a picture, the user is redirected to the listing's page. Here are some screen from the application in order to see the front-end developer in React:

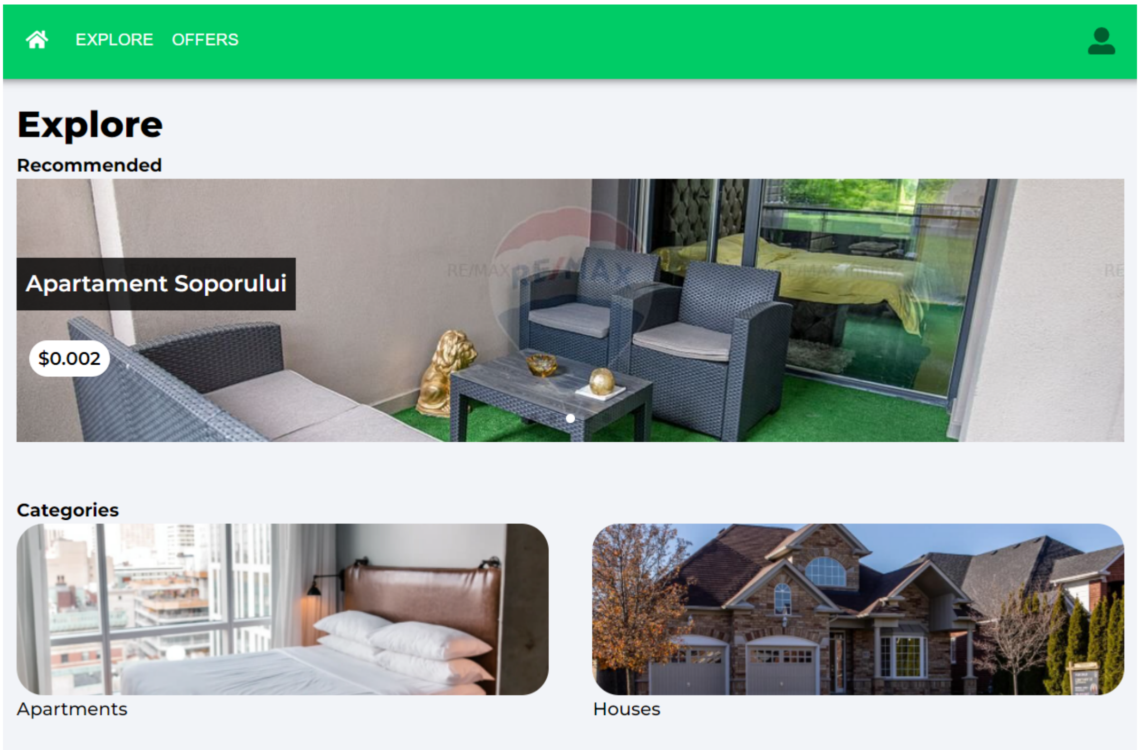


Figure 13: Main dashboard

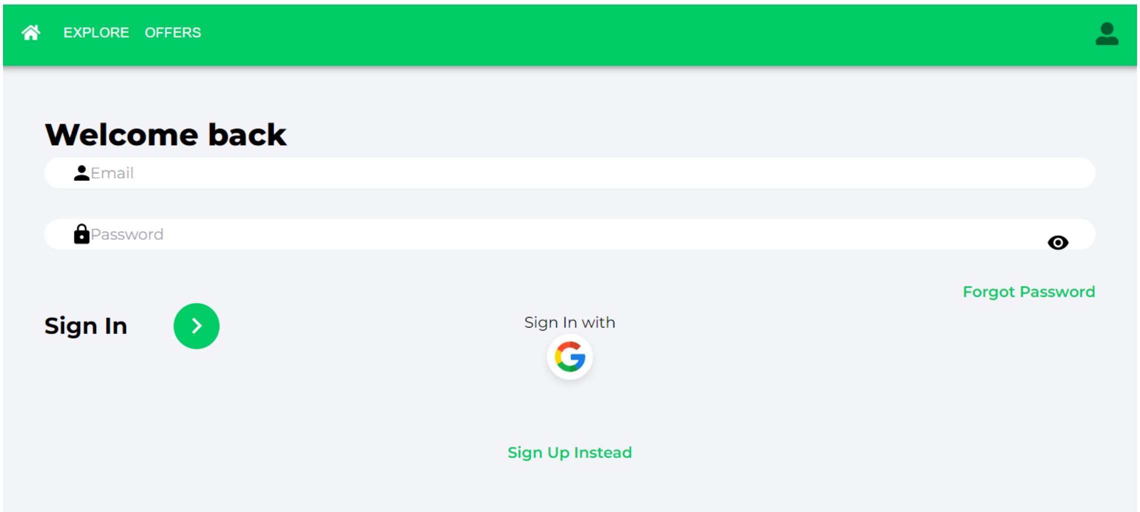


Figure 14: The login page

The next one is the buy listing page; here are details about the property, the navbar implemented with Material UI, the photos are inserted into a Swiper slider, the map is shown using the Leaflet library and the buttons for interacting with Ethereum are connected using ethers.js .

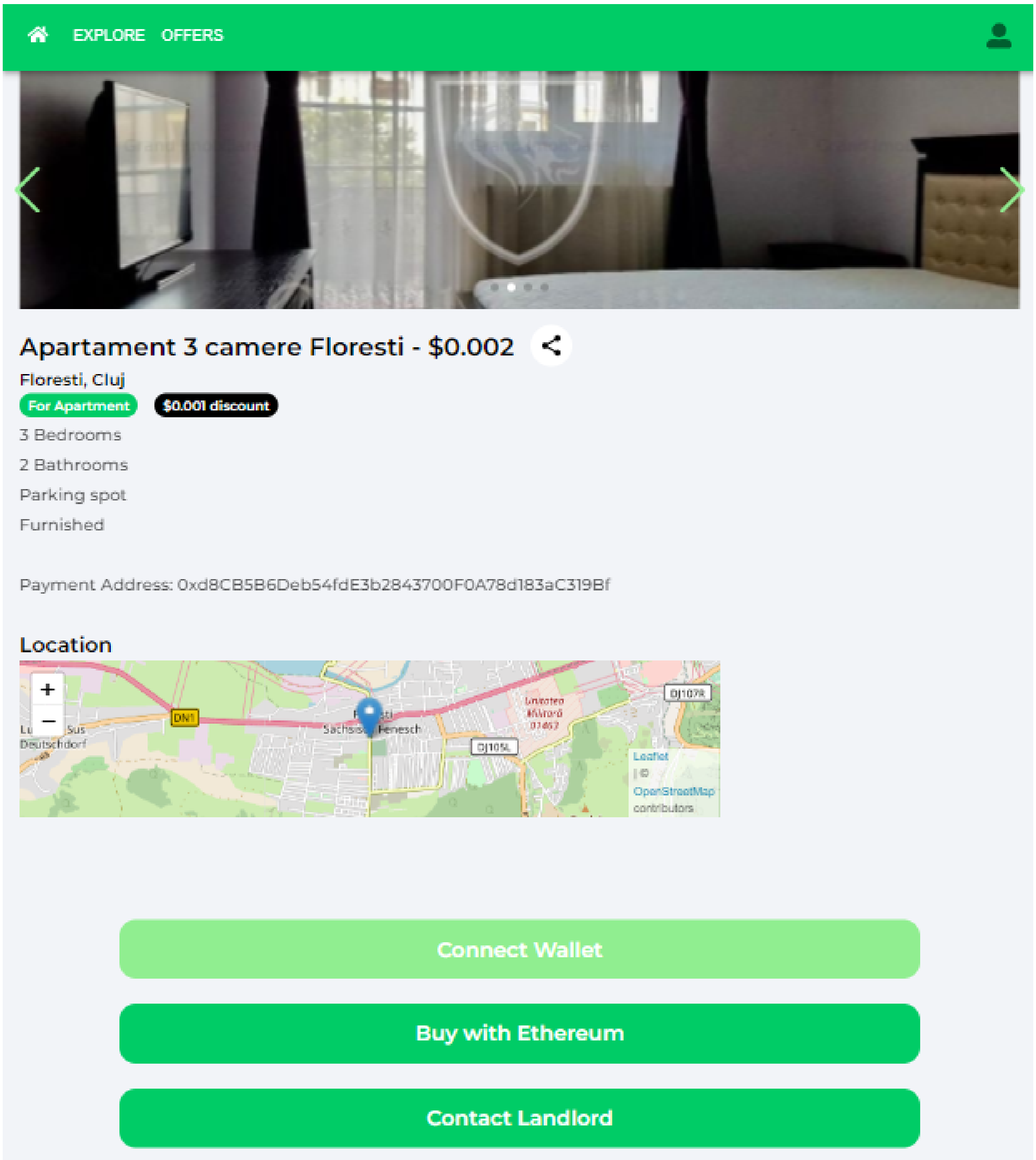


Figure 15: Listing page

4.3 Firebase

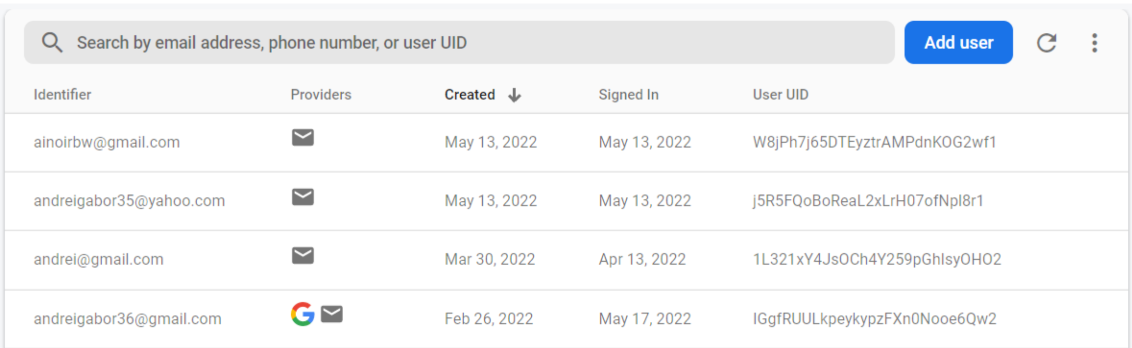
Backend-as-a-Service (BaaS) app development platform Firebase offers hosted back-end features such a realtime database, cloud storage, authentication, crash reporting, machine learning, remote setup, and static file hosting.

Firebase Authentication aims to make creating secure authentication systems simple while also enhancing end-user sign-in and onboarding. It offers an end-to-end identity solution that includes email and password accounts, phone authentication, and Google, Twitter, Facebook, and GitHub login, among other things.

Cloud Firestore is a flexible, scalable database for mobile, web, and server development from Firebase and Google Cloud. It employs realtime listeners to keep your data synced across client apps and provides offline support for mobile and web, allowing you to design responsive apps that function regardless of network latency or Internet access, just as Firebase Realtime Database. Cloud Firestore also seamlessly connects with other Firebase and Google Cloud products like Cloud Functions.

On the Firebase Authentication part there is a database which keeps an identifier - the email, the providers - email or / and Google account, the creation date, last signed in date and an auto-generated User UID. There can be added more Sign-in like Facebook, Linkedin or other social media platforms.

In the next picture, can be seen how the users are stored:


Search by email address, phone number, or user UID

Add user

Identifier	Providers	Created	Signed In	User UID
ainoirbw@gmail.com		May 13, 2022	May 13, 2022	W8jPh7j65DTEyztrAMPdnKOG2wf1
andreigabor35@yahoo.com		May 13, 2022	May 13, 2022	j5R5FQoBoReaL2xLrH07ofNpl8r1
andrei@gmail.com		Mar 30, 2022	Apr 13, 2022	1L321xY4JsOCh4Y259pGhIsyOHO2
andreigabor36@gmail.com		Feb 26, 2022	May 17, 2022	IGgfRUULkpeykypzFXn0Nooe6Qw2

Figure 16: Listing page

In the Firestore are kept the listings in a NoSQL manner. Data is stored in Firestore's "documents," which are included within "collections." Nested collections can also be seen in documents. Our users, for example, would each have their own "document" in the "Users" collection. We can use the collection method to refer to a collection within our code. For each of them is the number of bedrooms, the Ethereum address etc. There are also three indexes created for optimal data retrieval.

5 Conclusion

The potential effects of implementing a blockchain-based system in the real estate sector were investigated in this thesis. The study contributes to a better understanding of blockchain technology, including its potential and challenges in the real estate sector. The need of adjusting to rapid changes in regards to rising digitization was emphasized in the thesis in order to stay competitive in the market. The shift to blockchain-based systems is most likely one of these modifications that must be made in both the financial and real estate markets in order for actors to maintain long-term market positions.

The real estate sector could be transformed by blockchain, with fewer inefficiencies. Personal biases could be addressed and rectified, and a more liquid market could emerge as a result of lower transaction costs. With more openness, real estate cycles and market volatility could be reduced. One of the most significant obstacles to a seamless adoption of a blockchain-based system is a fundamental shift in people's perceptions of property worth and trust in digital systems. One of the system's most significant advantages is its high level of security and unhackability, making it difficult to corrupt and defraud the system.

As previously said, the introduction of blockchain could help to more transparency and openness inside the system, but it will come at a cost to the general population. The businesses will most certainly change their business models, but they will still make a lot of money. Companies will begin to take responsibility for their enhanced transparency in some way, which may result in less competition, higher prices, and increased market dominance.

The platform presented in the last part of the thesis could help the blockchain adoption to all people, make transactions more secure and faster. Also, it can be very useful in the third world countries, where people do not have documents for all the properties. The real estate market is on the verge of a huge technological shift thanks to new technologies like smart contracts and crypto mortgages.

References

[Ash73] E. Ashtor. Banking instruments between the muslim east and the christian west. *Journal of European Economic History*, 1:553–573, 1973.

[Blo] Metro Atlanta Blog. Selling a home in metro atlanta.

[CHE21] JAMES CHEN. Real estate, 2021.

[coi12] Total market cap, 2012. 28 April 2022.

[Con22] Alec Concejero. The future of real estate: Blockchain technology in real estate transactions, 2022.

[Cro15] Nachiappan Pattannayak P. Kalayanaraman V. Crosby, M. Blockchain technology: Beyond bitcoin. *Sutardja Center for Entrepreneurship Technology Technical Report*, 2015.

[DC17] Ulrika Lindh Denis Corluka. Blockchain - a new technology that will transform the real estate market. 2017.

[DEV22] ETHEREUM TOKEN DEVELOPMENT. Are you aware of how to create your own ethereum token, 2022.

[FVS16] Jesús Fernández-Villaverde and Daniel Sanches. Can currency competition work? *NBER Working Paper*, 2016.

[HS18] Faiza Rizwan Husneara Sheikh, Rahima Meer Azmathullah. Proof-of-work vs proof-of-stake: A comparative analysis and an approach to blockchain consensus mechanism. *International Journal for Research in Applied Science Engineering Technology (IJRASET)*, 6, 2018.

[J.16] Miró G. J. Strategic innovation in financial sector: Blockchain and the case of spanish banks. 2016.

[JLL] JLL. The global real estate transparency index.

[KOS18] MAYA KOSOFF. Bitcoin bros cameron and tyler winklevoss can't catch a break, 2018.

[Moh18] Debajani Mohanty. *Ethereum for Architects and Developers With Case Studies and Code Samples in Solidity*. Apress, 1 edition, 2018.

[Nak08] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[Rob] Regan Robillard. Smart contracts.

[SAS19] Ledger SAS. What is proof-of-work, 2019.

[SH91] W. Scott Stornetta Stuart Haber. How to time-stamp a digital document. 1991.

[VAR22] ZOLTAN VARDAI. What is opensea and why is everyone talking about it?, 2022.

[VD19] H. Badis V. Deshpande, L. George. Safe: A blockchain and secure element based framework for safeguarding smart vehicles. *12th IFIP Wireless and Mobile Networking Conference (WMNC)*, 2019.

[Wil17] J.B. Williams. *The Electronics Revolution: Inventing the Future*. Springer, 1 edition, 2017.

[Yak19] Anatoly Yakovenko. How solana's proof of history is a huge advancement for block time, 2019.