Tokenized Property Renting and Trading Using Blockchain

by

Md. Miraj Hossain
18201003
Kazi Sazid Ahmed
18201025
Senjuti Saha
19101080
Kazi Tasmima Eshan
19301032
Tasmia Akand
19301022

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
September 2022

Approval

The thesis/project titled "Tokenized Property Renting and Trading Using Blockchain" submitted by

1. MD Miraj Hossain (18201003)
2. Kazi Sazid Ahmed (18201025)
3. Senjuti Saha (19101080)
4. Kazi Tasmima Eshan (19301032)
5. Tasmia Akand (19301022)

Of Spring, 2023 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on May 29, 2023.

Examining Committee:

Supervisor:
(Member)

Md. Sadek Ferdous

Dr. Md Sadek Ferdous

Associate Professor

Department of Computer Science and Engineering

BRAC University

Program Coordinator:
(Member)

Arif Shakil

Lecturer

Department of Computer Science and Engineering

Brac University

Head of Department:
(Chair)

Dr. Sadia Hamid Kazi

Chairperson

Department of Computer Science and Engineering

Brac University

Abstract

It is challenging for any authoritative figure to keep track of and oversee the house rental market because of the large number of landlords, arbitrary fees, misleading rental information and other issues. On the basis of Blockchain technology of encryption algorithm, this paper develops a property buy, sell and rental system. The system uses smart contracts to form all kinds of agreements, establish the relationship among users, pay and collect rent automatically on a regular basis and return the rental right when it is due. With this approach, there is no need for mediation, it is less expensive, rental information is transparent and it is easier to keep track of all the records for an authoritative figure using this system.

Key Words: Blockchain, Tokenization, Smart Contract, NFT, Real Estate, Property Trading, House Rental.

Declaration

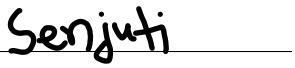
It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Md Miraj Hossain
18201003

Kazi Sazid Ahmed
18201025



Senjuti Saha
19101080

Kazi Tasmima Eshan
19301032

Tasmia Akand
19301022

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

From the very beginning till the date, one of the most basic needs of the human race is shelter. In recent years, after the rising tension of war and the devastating fall of the financial situation of the world, homeownership has become very much unfeasible. In order to make this basic need feasible and in everyone's reach, we're opening a platform which will make capitalist people invest in real estate, and the renters to rent a single room or multiple rooms even the flat as a whole in accordance with their needs and ability of affording. Consequently, to make the entry point of the housing market more accessible, credible and customer-friendly, we have come up with the idea of tokenizing, renting and leasing a part of a house or the whole. In this regard, the concept and technology of blockchain tokenization will be used to represent the new model of equity sharing through which home renters can more easily obtain the necessary requirements.

Blockchain is comparatively one of the new concepts in the security industry in which a distributed ledger is used to store the necessary information and the history of transactions which is at the same time completely transparent to both parties. It is growing each day in an exponential manner as people are being attracted by its powerful security mechanism which is making them implement the system in their security models. According to the most recent research report, the size and share of the worldwide blockchain technology market were estimated to be worth USD 4.8 billion in 2021 and are predicted to reach USD 69 billion by 2030, growing at a CAGR of almost 68 percentage from 2021 to 2026 [1]. To be more specific, we are using the approach of property tokenization through NFT also known as non-fungible-token meaning that a property or an asset is tokenized with a specific token which is unique forever and non-duplicable. In the field of real-estate or relevant areas, it can play a momentous role to ensure security and attain beliefs of both investors and renters as real-estate is one of those areas where people have been facing loads of defraudation.

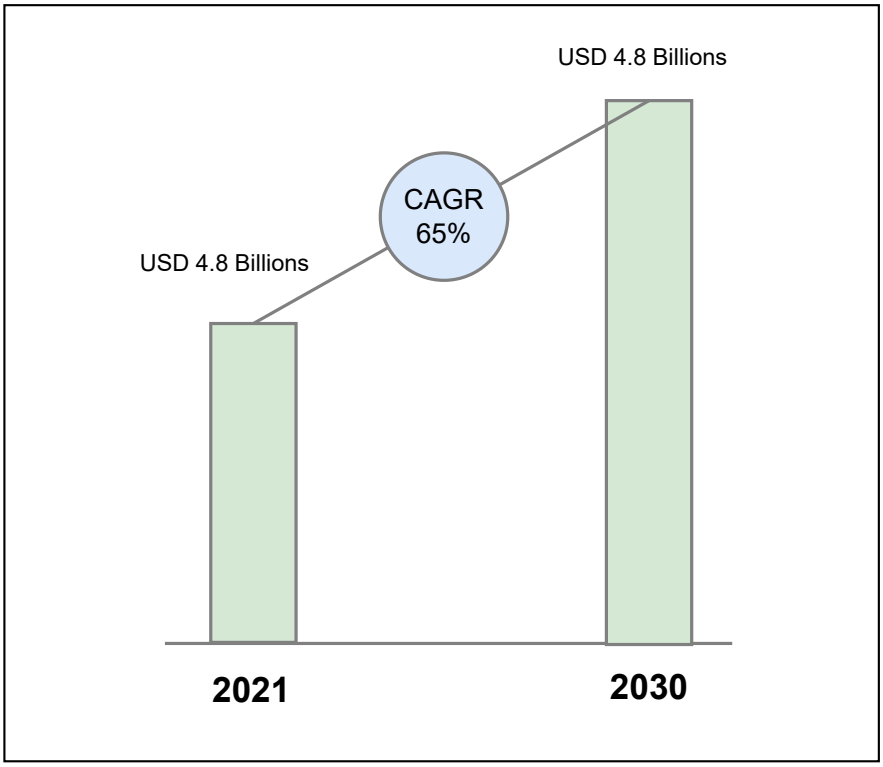


Figure 1.1: Global Blockchain Technology Market

Hence, we are particularly interested in bringing an ease in this sector making a convenient setting for both the investors and the customers. In addition to this, since blockchain based property tokenization requires the use of crypto-currencies to make the environment decentralised and it is not legalised in some developing countries like Bangladesh yet, we have been constructing the idea of dispelling this transacting issues by incorporating the idea of private blockchain for these countries so that our implementation would be fruitful to any part of the world.

1.2 Problem statement

While shelter is one of the basic needs of human beings, we witness a lot of different issues regarding this matter. With the rise of population and urbanisation, the need of renting a property according to one's need and potential, has become a crucial part of modern society. There are a heap of fraudulent and incommodious cases where both parties, the owners and the tenants face endless amounts of disastrous consequences because of the traditional unclear rental systems and agreements.

According to [2], an average property manager says that 15 percentage of their online rental applications contain evidence of blatant fraud, and the respondents predicted that a further 10 percentage of fraudulent applications go unreported. They have also mentioned its aftereffects which includes costs related to property damage on a physical level, missed opportunities to rent to quality tenants, alleged crimes on the property, and reputational damage of the owner.

Not only fraudulence but also there is risk of accepting cash payment like we always have to manually keep records or receipts of the payment [3]. If the receipt is lost somehow, it would create a great hassle for both parties. In case, tenants lose the receipt, they might be forced to pay that rent again for not having proper evidence. In an opposite scenario, tenants might take advantage of the situation and falsely claim that they have already cleared their rent if the landlord loses their receipt and fails to provide evidence.

Another risk of accepting cash payment is its vulnerability to robbery [3] . To be more specific, tenants or any person with ill-intention might track down the deposit activities of the landlord which can make him prone to robbery or theft. Also, proper management of tangible cash is very inconvenient to carry out.

There are incommodious cases where tenants are convicted forcefully due to the owner's selfish motive or nepotism [4]. In some cases, it is seen that tenants are suddenly told to leave their house without taking any prior consent which is against the law according to Act 1991 Section 18 [5].

There is another concern for the tenants that there might be a sudden rent increase against "The Premises Rent Control Act 1991" [5]. Over the years, there are many cases where owners increment the rent without taking the law into consideration and the result is that in Dhaka city, house rent has increased between 14-21 percent [5]. Also, according to [5], tenants are asked to pay two months worth advance by their landowners which is another violation of law.

In this research work, we will attempt to dispose of these matters by implementing the algorithms of Blockchain technology specially NFT, which will create a user-friendly, permeable and easy to operate system. To do so, we are looking forward to operating a digital transaction system to make it a distributed platform and maintain the transparency but, we have observed that including Bangladesh there are many developing and also least developed countries, in which digital transactions such as crypto-currencies are still not allowed.

As reported by the Foreign Exchange Regulation Act 1947, the Money Laundering Prevention Act 2012 and the Anti-Terrorism Act, 2009, any type of virtual coin or cryptocurrency cannot be maintained or traded in the country (Bangladesh) [6]. However, we are conducting our research to find a solution to lessen these hassles and make it available for all the people over the globe.

1.3 Research Objectives

The purpose of this research is to design a system through which the online renting process of a flat or a single room will be much user friendly, secured, cost efficient and transparent. A rental system without blockchain and NFT is prone to fraudulence. Hence, we are aiming to design our system in a way that will ensure the rental-owner of a specific flat or room is one person at a time using NFT. Furthermore, the transaction and rental availability status will become transparent. The objectives of this research are:

- **RO-1:** To clarify the basic concepts of blockchain, tokenization and property tokenization.
- **RO-2:** To study related literature works and existing commercial platforms.
- **RO-3:** To find out the overall as well as region specific challenges we would face while implementing our idea and think of probable solutions.
- **RO-4:** To identify the requirements for the development of our system.
- **RO-5:** To design the architecture and protocol flow of the system.
- **RO-6:** To solve the challenges and develop the proposal accordingly.

1.4 Report Structure

In this thesis, we have developed mainly eight chapters including Introduction, Background, Related Work, Proposal, Data Model, Implementation and Conclusion. Besides, we have Abstract, table of contents, list of tables, list of figures and References.

To begin with, the first chapter namely introduction consists of motivation which reflects our main motivation for this research, our primary idea as Problem Statement, Research Objectives and a short overview of this report. In the Problem Statement part, we have addressed the different existing problems regarding traditional rental systems along with the territorial challenges we would face while implementing our system. Next, the Research Objectives part has six explicit policies we have set for accomplishing our goal gradually.

Next in the second chapter, we have explained the main technologies and concepts we will use while developing our research such as Blockchain, Ethereum, Tokenization and finally, Property Tokenization.

The third chapter is Related Work in which we have discussed some of the research papers related to our topic, their summary, the concepts used in those papers etc. Also, we have given ideas on some running commercial websites based on our research interest in this section.

In chapter four, we have constructed our research proposal, threat model, requirement analysis and discussed the architecture briefly.

In chapter five, we have presented our data model and explained it. We have catagorized our request and response data separately. Also, thoroughly discussed how they have been used in the report.

We provided and covered the entire protocol flow and implementation in chapter six. We have presented the primary user interface of the system and explained all the procedures.

In chapter seven, we have the analysis and discussion section where we have presented some analysis as well as discussed the advantages, limitations and future

works of this system.

We concluded briefly having a short discussion over the whole report and by outlining our future work intentions in chapter eight.

Chapter 2

Background

2.1 Blockchain

Blockchain offers a safe, decentralised mechanism to track and transfer asset ownership. The real estate business might undergo a revolution as a result. This technology has the potential to significantly alter how real estate transactions will be conducted in the future. Blockchain is a type of shared database that differs from a regular database because it saves data in blocks that are then connected via cryptography [7]. Each time new information is received, a new block is created and filled with it. Data is chained together in chronological order once a block has been filled with information and is then chained onto the block before it. A blockchain can be used to store various kinds of data, but up until now, transaction ledgers have been the most widely used application. Blockchain is employed in the context of Bitcoin in a decentralised manner, allowing all users to collectively maintain control rather than any one person or organisation. Since decentralised blockchains are immutable, the data entered into them cannot be changed. This implies that transactions made using Bitcoin are publicly visible and permanently recorded.

2.1.1 Distributed Ledger Technology (DLT)

DLT is a decentralised database that is governed by numerous users on various nodes. A hash, an immutable cryptographic signature, is used to record transactions on a blockchain, a type of DLT. The subsequent grouping of the transactions into blocks, with each new block containing a hash of the preceding one to chain them together, is the reason why distributed ledgers are frequently referred to as blockchains. Table 2.1 is a tabular representation of DLT properties along with its advantages.

Property	Advantage
Distributed	For complete transparency, a copy of the ledger is available to all network user.
Immutable	Any validated records can not be changed.
Time stamped	A transaction time stamped is recorded on block.
Unanimous	All network participants agree to the validity of each of the records.
Anonymous	The identified participants are either anonymous or pseudonymous.
Secure	All records are individually encrypted.
Secure	All records are individually encrypted.
Programmable	A blockchain is programmable such as: smart contract.

Table 2.1: Representation of DLT properties along with its advantages

Transaction

A chain of unbreakable blocks is formed between transactions. The verification of each subsequent block, and subsequently the blockchain as a whole, is strengthened by each new block. By giving the essential strength of immutability, this makes the blockchain tamper-evident. As a result, there is no longer a chance of malicious actors interfering with the ledger and other network members may have trust in it. Transaction adding mechanism is illustrated in Figure 2.1.

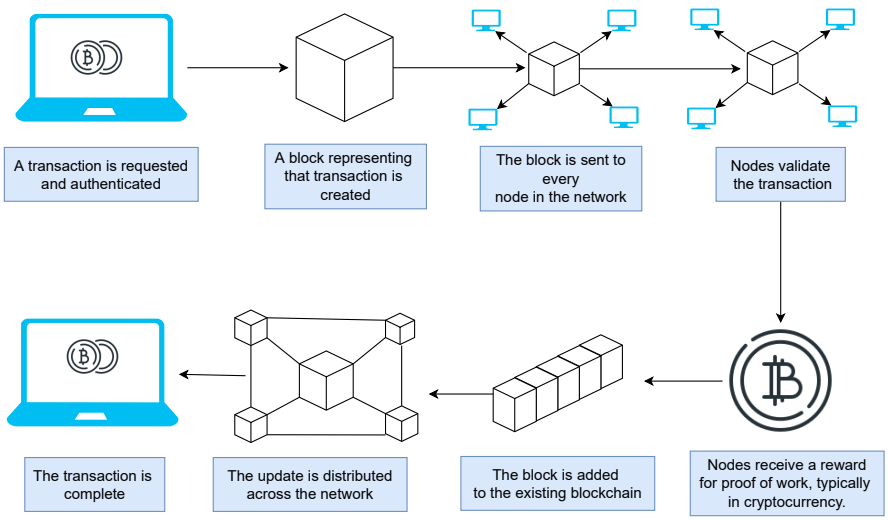


Figure 2.1: Transaction adding in blockchain

- **Authentication:** Using Cryptographic keys (public key and Private key) users are identified and given access to their account or wallet. The public key is known to all just like an email address, whereas the private key is known to the user only which is used to generate a digital signature of the user. Therefore, using these both types of keys faithfully helps to authenticate any user as one cannot spend the money sent to him without his own private key.

- **Consensus algorithms:** A consensus algorithm is a process that allows every participant in the Blockchain network to agree on the current state of distributed ledger. It is treated as the most fundamental part of blockchain technology as it is what blockchain network achieves its security, transparency and immutability for, not having a central authority though. However, we have several consensus algorithms; but among them Proof of Work(PoW) and Proof of Stake(PoS) are the most familiar and effective ones. In the following, we present a short introduction of these two algorithms.

- **Proof Of Work (PoW):** To reach the above mentioned consensus, it is needed to use a protocol which is known as Proof of Work protocol where a network of participants tries to solve a complex mathematical problem not only to make the transaction valid but also to add the transaction to the block. This process is called mining and the miners, whoever can solve the problem, are rewarded with new crypto-currencies [8].

- **Proof Of Stake (PoS):** Another protocol to reach consensus is proof of stake which is a later and advanced consensus mechanism of PoW. It requires a number of participants who must have a stake in the blockchain - usually having some of the crypto-currencies in their hands. The participants here are called validators who checks transactions, verifies activity, votes on outcomes, and maintains records. Unlike PoW, it doesn't require complex computational power among the validators but a certain amount of coins instead [9].

  In this manner, a successful transaction requires all these key steps to go through to be a valid transaction and finally, added to the blockchain.

2.2 Cryptocurrency

Cryptocurrency is a form of digital or virtual currency that uses cryptography for secured financial transactions and controls the creation of new units, and verifies the transfer of assets [10]. It is a decentralized system that operates on a technology called blockchain, which is a distributed ledger that records all transactions across the network. There are over 200 existing cryptocurrencies [11]. Some widely used cryptocurrencies are Bitcoin(BTC) [12], Ethereum(ETH) [13], Tether(USDT) [14], Binance coin(BNB) [15] and many more.

2.3 Ethereum

Ethereum is mainly a global software platform that establishes a peer-to-peer network on the decentralised blockchain system [16]. It natively supports smart contracts which is considered as one of the key features of Ethereum. One of the widely used cryptocurrency of this platform is ethereum (ETH). The smallest unit used for this currency is called gwei. In Bangladesh, 1 ethereum converts to 194,351.38 BDT and 1 gwei = 0.01947450 BDT.

2.3.1 Smart Contract

An application that runs on the Ethereum blockchain is defined as a smart contract. It refers to a predefined set of rules, agreements and data that are stored at a particular address on the Ethereum blockchain. Once specified predefined conditions are met, it can execute transactions autonomously without the aid of an intermediary entity [17]. In addition, it works in the same way as a traditional contract, the only difference is that traditional contracts are enforced by law whereas smart contracts are enforced by those predefined codes which makes the contract works in a really smart way. However, the best feature of a smart contract is that after a transaction has been completed, its ledgers can never again be tampered with or changed by any party. In light of this, smart contracts are regarded as trustworthy for transactions requiring stakeholder anonymity, transparency and confidence.

2.4 Tokenization

Tokenization (Figure 6.5) is the process of turning sensitive information into anonymous, non-sensitive data that may be utilised in a database or internal system without putting it at risk. A token is a piece of information that represents a more important piece of data. The purpose of tokenization is to protect sensitive data while preserving its business utility [18]. The only reason tokens are helpful is because they stand in for anything valuable, such as a credit card primary account number (PAN) or Social Security number (SSN) [19]. In order to making tokenization operate, the useful data in your environment must be removed and replaced with these tokens. Whether it is credit card information, personal health information, Social Security numbers or anything else that requires security and protection, most organisations store at least some sensitive data in their systems. Organisations can continue to use this data for business purposes by tokenizing it, minimising the risk and compliance requirements associated with maintaining sensitive data internally.

However, the objective of a successful tokenization platform is to preserve the original data in a secure cloud environment that is separate from any organization's system, exchange each data set for an uncrackable token and remove any original sensitive payment or personal data from the IT infrastructure of the organization. For instance, tokenization in banking secures cardholder information. Only the original credit card tokenization system has the ability to swap the token with the matching main account number (PAN) and submit the information to the payment processor for authorization when you process a payment using the token stored in your systems. Only the token is recorded, sent or stored by your systems; never the PAN.

2.5 Property Tokenization

Property tokenization (Figure 2.2) is a way to securitize our real world assets by dividing it into several digital tokens. These digital tokens are often called "security tokens" which represent a portion of the predefined asset and by buying these tokens one will own a portion of the equity in that asset. It should be noted that security

tokens are secured using the immutability of blockchain technology and tradeable via crypto exchanges or alternative trading systems. In addition to that, the predefined conditions for the tokenized property are stored in the "smart contract" which will be implemented automatically without any human intervention. By purchasing these tokens, investors can gain unique access to real estate assets with transparency and liquidity. There are three distinctions of tokens according to their features - utility tokens, payment tokens and asset tokens. Again, based on asset type, property tokenization can be divided into four categories such as Commercial, Residential, Single and Trophy property tokenization.

To tokenize a property, we need to achieve three fundamentals. Firstly, finding a properly regulated blockchain platform. Secondly, to make sure the platform allows ownership transfer facilities in a legitimate manner. Thirdly, assuring that tokens can be traded at a given price so that each share of the property can have its actual value reflected in tokens. If all the standards are satisfied, the property will be tokenized, and the owners will have the option to choose the number of digital tokens that will be created from their actual property and made available for trading on their respective platforms. Apart from this, property tokenization lowers the overall cost of a real estate investment by cutting out the intermediary and utilising automated smart contracts. Property tokenization not only reduces costing but also solves the illiquidity issue of real assets. The process of fractionalizing the whole property into smaller tokens, enables the owners to offer it at a lowest possible cost resulting in a tremendous chance for the small investor to take part in the investment market. Hence, property tokenization can eradicate the existing global or regional barrier in the real estate market.

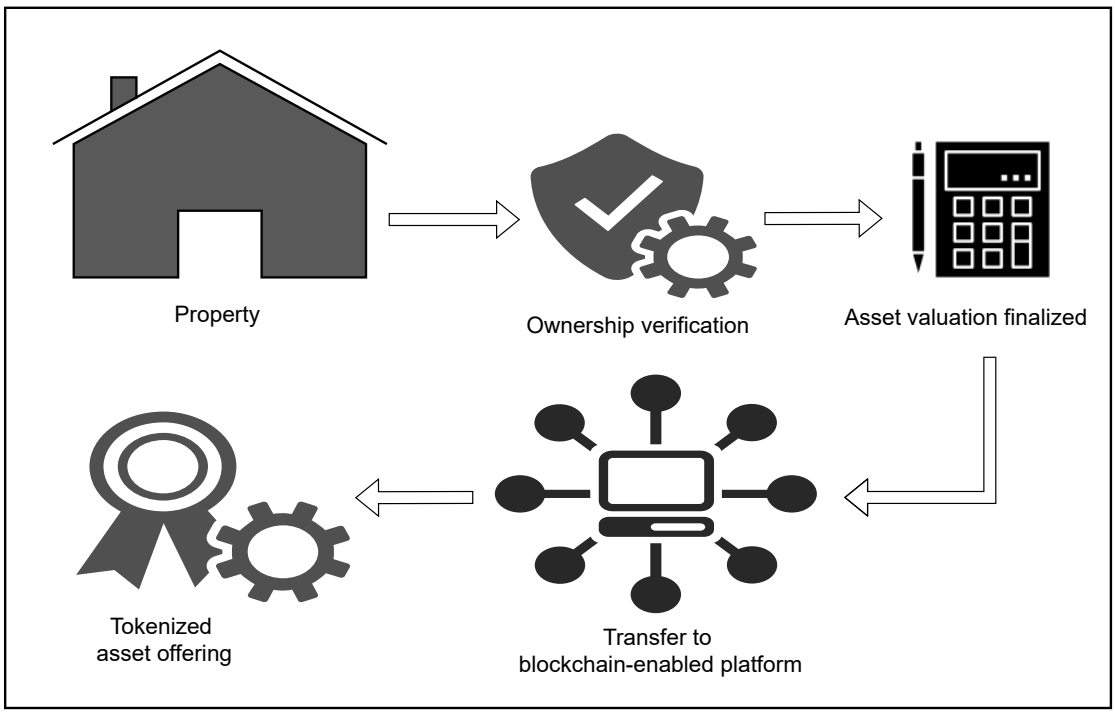


Figure 2.2: Property Tokenization Process

Chapter 3

Related Work

In this section, we have discussed some related works and commercial platforms related to our research interest.

In this study [20], they make use of data from a US-based business that has so far concentrated on opening up US residential real estate to investors via the Ethereum blockchain. The company name is RealT. In accordance with US regulations, the corporation buys residential properties and tokenizes the legal entity in possession of the property's deeds. It hires a third party to manage, maintain, and collect rent from the properties. Investors can move a property's tokens to other wallets after buying one or more of them. The wallets that buy the tokens need to be on the company's whitelist since there are legal and compliance restrictions on who can possess them. Right now, the only way to get on a whitelist for a property is to purchase at least one token for it on the management company's website. Each investor has a contract with that particular limited liability corporation because each property is a separate entity.

This paper [21] is a critical analysis of the future of tokenized real estate investing and discusses both the benefits and potential long-term risks of tokenizing real estate. In the first chapter Andrew Baum started discussion with two issues faced while considering real estate as an asset, the first of which is illiquidity and the second of which is lumpiness. In addition to that, he also suggested crowdfunding as a potential solution to the issue of purchasers needing funds and as a means of removing geographical constraints to capital raising. He also mentioned the failings of the peer-to-peer lending and crowdfunding marketplaces. Additionally, it illustrates the beneficial impact of digitised real estate on capital raising as well as his scepticism regarding its impact on fundraising. Overall, the first chapter makes it quite evident that, while there are potential uncertainties, a thorough implementation of digitised real estate can resolve the problems of illiquidity and lumpiness. The following chapter of Andrew Baum's report is where he analyses various forms of fractionalization and their legal ramifications. He asserts that fractionalization is advantageous to those who favour partial ownership rather than those who are only interested in full ownership. He then discusses fund structures and details fractionalization's historical failures. He has also included a succinct overview of the most recent effort to fractionalize an asset, IPSX. In this discussion, he talked about its system, advantages, direct retail investors as their target investors and who will be

their sellers after comparing the pricing with the private sale process. Apart from this, he mentioned two issues with IPSX - the first one is a regulatory issue and the second one is that what they are selling is not the same as what they are promoting. He expects IPSX to benefit from the political unpredictability of 2019, which was a challenging year for equity capital markets. He then moves on to chapter three, where he proposes tokenization of fractional property. Our author concentrates on tokenizing fractional property for the remainder of the report because tokenization of intellectual property is already regarded as successful. Additionally, he spoke on the potential for tokenization to emerge in the future as a result of developing blockchain technology. The fourth chapter goes on to explain security, utility, and hybrid tokens as well as how they interact with fractional property. Additionally, he discusses the intermediate structure of the tokenization of debt, funds, and individual assets. S&P Global Market Intelligence, Jakob Drzazga's statements about his own sources of inspiration and the difficulties he encountered while establishing Brickblock are also included in the report. Drzazga mentioned the systematic errors and overall regulatory issues as challenges as well as expressed his concerns for which at least for now he is not going to focus on other parts of the real estate sector. He discusses token regulation, related concerns, and how tokenizing intellectual, virtual assets is considerably simpler than tokenizing physical assets in the chapter that comes next. The author asserts that there aren't any significant tax, accounting or valuation issues that could stifle the development of tokenized real estate securities in the next section. On the other hand, it is quite improbable that a secondary market will offer sufficient liquidity, which significantly lessens the appeal of tokenization for specific real estate investment assets. He explains various successful tokenizations with evidence from FIBREE in the following two chapters, as well as some failures, and predicts that there will be a number of innovations if tokenization gains popularity. The author came up with the conclusion that tokenization is still in its early stages, with intriguing prospects as well as the possibility that innovation will be delayed by several years or decades.

The following research paper [22] investigates the application of security tokenization to commercial real estate assets and it is believed that the tokenization of physical assets for the purpose of standardised, transparent, and tamper-proof record keeping has the potential to create significant value for investors in securities that derive their intrinsic value from real, physical assets. It is clear that there are benefits to using blockchain for securities trading. The tokenization provides a broad foundation for future research on the tokenization of various asset classes and the securities that are linked to them and make references to real, fixed assets. Real estate, a notoriously illiquid asset class, demonstrates a number of characteristics that blockchain claims to solve for other types of securities, including new methods of funding, more liquid markets, tamper-proof ownership histories and simplified payments. The paper also examines three areas where blockchain technology is being used in real estate: (1) the issuing and trading of securities, (2) the value chain for real estate investments and (3) the depiction of the actual physical assets themselves. In this application, the use of blockchain in loan origination and servicing will assist downstream investors, who will be able to track a loan's whole lifespan from issuance to maturity. It is noticed that a growing number of layers and procedures in the trading and compliance process are being applied to blockchain in

the initial stage of securities tokenization. Here, the development of blockchain is based on infrastructure for digital identity which include the identity of people and of things. In this research paper, we were able to create a variety of lines of inquiry that revealed the information most crucial to our comprehension of the opportunities and difficulties associated with implementing tokenization in the commercial real estate sector. In other words, it's not only about tokenizing equities; it's also about tokenizing physical assets which will have significant advantages that can be realised.

Apart from the research papers, we also have studied some existing platforms which are also based on blockchain technology. Following (Figure 3.1) is a short overview on some of them:

Propy	A property purchasing platform. Location: Palo Alto, USA Founded: 2015 Money raised: $15 million Blockchain Platform: Ethereum Data Stored: BlockChain
Harbor	A platform for tokenizing private securities. Location: San Francisco, USA Founded: 2017 Money raised: $38 million as of April 2018 Data Stored: in three ways- 1)Stored in blockchain 2)Stored in their own server 3)Stored within data provider servers (agencies or vendors) Security System: uses Ethereum's ERC20 based regulated tokens (R-Token).
BitRent	The first blockchain real estate platform, it links investors and property developers. Location: London, UK; Prague, Czech Republic. Founded: 2016 Money raised: $180 million as of 2017 Data Stored: Blockchain.

Table 3.1: blockchain based real estate platforms

Chapter 4

Proposal

4.1 Proposal

Our proposal is developing a transparent distributed rental and trading platform from where people can rent, buy and sell a property in accordance with their necessity. In particular, we will focus mainly on implementing the system using NFT tokenization so that the system will run smoothly without any intermediary hassle. Here, the investors who are the owners of a residence will have the feasibility of tokenizing their assets for further exposition and making advertisements. As a consequence, the people who are interested in trading (buying, selling and renting) a flat will have the scope to pick their preferences from a list full of diverse options, also with a validity per their desire.

The main challenges in this sector are so many to describe among which the most important ones we have demonstrated in the section of Problem Statement according to some website sources. However, to realise our proposal, we will be going through the following steps:

- **Threat Modelling:** To strengthen the security of this system and mitigate all the vulnerable threats, we will try to picturesque all the possible threats following a widely used model. We will find the possible potential threats and categorise them accordingly.
- **Requirement Analysis:** To carry out the reasonable solution of the existing problems, we will work on the functional specifications, privacy requirements and so on. To do so, we need to understand the expectations of the users and their struggles to make it a proper user-friendly and secured platform.
- **Architecture design and Protocol Flow:** After analysing the requirements, we will focus on the architecture design and protocol flow. We want to design our research marketplace in such a way that users find it convenient to use and thus we will be able to solve the conventional problems in this sector.

4.2 Threat Modelling

We have designed a structured threat model in order to guarantee the high level security development of our system. This model makes it easier to recognize the numerous security risks that might be posed to our system. Below, we have implemented Microsoft's STRIDE **r15**, threat model.

- **T1-Spoofing:** The most known type of spoofing is probably email spoofing which also include cookie replay attacks, session hijacking, and cross site request forgery (CSRF) attacks. For example, spoofers might attack the rent owner's password/private key and illegally participate in the transaction. Hence, the transacted amount will be lost. In a severe scenario, if the administrator's password is cracked then the whole system might get out of control.
- **T2-Tampering with Data:** This attack violates the integrity. For example, attackers might attempt to tamper with the database of our website to cause unnecessary trouble.
- **T3-Repudiation:** A repudiation attack occurs when an application or system does not have controls to correctly track and log users' actions, allowing for malicious manipulation or forging the identification of new actions. An attacker might delete a whole purchase transaction information or any other sensitive information from the database.
- **T4-Information Disclosure:** Information disclosure violates the confidentiality of the system by revealing excessive information along with the necessary one's. This may occur as a result of developer comments left in the application, source code that contains parameter information, or error messages that reveal excessive amounts of information. This may lead the attackers to steal private information of our customers for their benefit or to cause trouble. Also, they might try to steal sensitive data from the system to sell them to our competitors for their profit.
- **T5-Denial of Service(DoS):** The most common form of DoS attack is a buffer overflow attack which simply sends too much traffic to the application, triggering a crash, and shutting it down to legitimate traffic. For instance, attackers can disguise themselves as fake customers to initiate conversations to create unusual traffic in the system so that legitimate users can not get in.
- **T6-Elevation of Privilege:** When an application acquires privileges or powers that are not appropriate for it, this is known as an elevation of privilege. Using a compromised account that already exists, an attacker tries to get more rights or access. For instance, an attacker may hijack an ordinary user account on a network and attempt to get root access or administrative privileges.

We have presented an analysis of the functional, security and privacy requirements for our system in this part. While security and privacy requirements are how we are protecting our system from the threats identified in the prior threat model, functional requirements here are the fundamental functionalities of our system. Below, we have discussed all these requirements respectively.

4.3 Requirement Analysis

4.3.1 Functional Requirements

- **FR-1:** It should be a platform where the owner can offer to rent their flats and the renter can easily get those rentable flats.

- **FR-2:** The users should be able to create a profile id with valid information and can have a unique user id.

- **FR-3:** The system should be integrated with a decentralized infrastructure so that the system cannot be controlled by a person or a group of people.

- **FR-4:** It should have a peer-to-peer transaction system.

- **FR-5:** It should have a tokenization system where the user or the owner can tokenize their transactions.

- **FR-6:** The system should be trustable. In these cases, the transactions should be transparent and immutable.

4.3.2 Security Requirements

- **SR-1 :** The application must be implemented with a strong authentication system like two factor authentication or email verification to mitigate the spoofing threat stated in T-1.

- **SR-2 :** The application should be designed to ensure the integrity of the data stored in the server. This will mitigate T-2.

- **SR-3 :** The application should take digital signature of users as proof of actions to mitigate any repudiation attack discussed in T-3.

- **SR-4 :** All the sensitive data should be encrypted during transmission and storage to mitigate T-4.

- **SR-5 :** The system should use a distributed system as well as a distributed database to mitigate T-5.

- **SR-6 :** There must be a strong access control mechanism to stop attackers from elevating their access control privileges and mitigate T-6.

4.3.3 Privacy Requirements

- **PR-1:** Before sharing any sensitive data or making transactions, the system must take consent from both entities.

4.4 Architecture

The current housing rental market is plagued with numerous problems since it lacks enough transparency, and reliance on paper-based contracts make it more vulnerable to fraud. In order to address these issues and alleviate the hostile relationship between tenants and landlords, we designed a blockchain and tokenization based renting system. A blockchain-based leasing system provides high-level security and privacy while being simpler, faster, and comparably cheaper. Additionally, this eliminates mediation offering transparent and immutable rental information.

In our designed system, any user can visit the website and take a tour. Whenever someone wants to provide their property or wants to rent, they will have to sign up or register themselves accurately with valid information. Here, Confidential information will be stored in the public blockchain and less sensitive ones will be in IPFS. Also, there will be a wallet along with the user's profile. The whole transaction will be managed automatically by the Ethereum wallet and codified rules in the smart contract. We have presented the architecture design of our system in Fig. 4.1. The whole architecture design is discussed here, splitting into three main parts DApp, IPFS, Public Blockchain. Now, we will be discussing how these three main parts are synergizing altogether and functioning to complete the whole system.

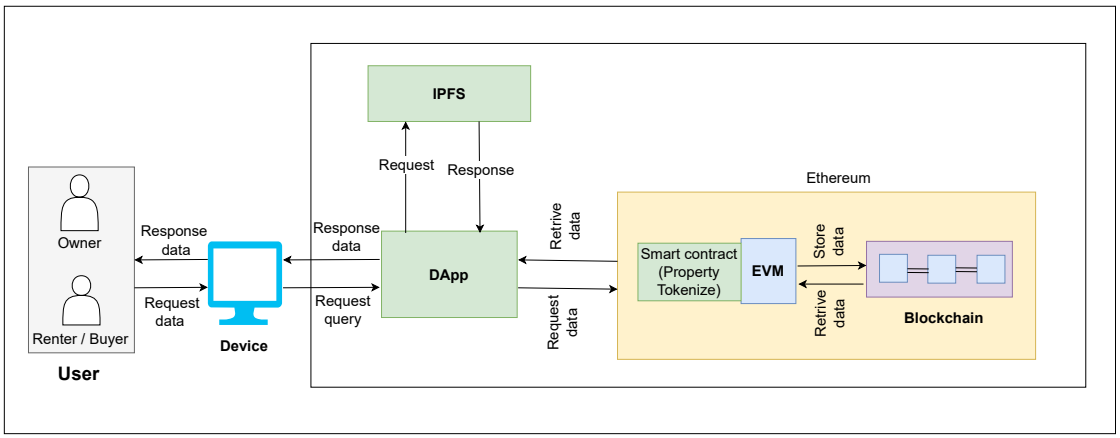


Figure 4.1: Architecture Design

4.4.1 User

User is the first entity of our designed architecture. Here, user can be a seller (owner of a prooerty), buyer or renter. To get any service, users interact with our system through their preferred devices(browser) with internet available.

4.4.2 DApp

DApps (Decentralized applications) are distributed, decentralized, open-source software programs that run on a decentralized peer-to-peer network in our property documentation system. The transition from the user interface to the blockchain platform is simple. Any user can tokenize their property on this system's user interface and sign in or up using their accurate information. A user will also have a specific profile, be able to examine their history, update their information, and give rent, among other services. Smart contracts on the blockchain will be used to store and retrieve all of the data. This DApp was created with Node.js and Express.js [23], [24]. Node.js is a popular server-side JavaScript platform for building DApps in the blockchain industry. Express is a Node.js web application framework used to create web apps. The necessary APIs for communicating with any Node.js application are provided by Ethereum. The DApp was created by us in a way that allows for system integration and enables it to support the aforementioned flow.

4.4.3 IPFS

Interplanetary File System (IPFS) is a distributed file storage protocol that allows for fast performance and decentralized data archiving. In our system, we are using IPFS to store comparatively less sensitive data (like- property pictures, price lists etc.) as they consume huge storage space. In public blockchain, this much storage will cost a lot and will make the system inefficient. Hence, we decided to choose IPFS along with public blockchain to make the storage use efficient, reduce the cost and make it work faster. Moreover, the IPFS protocol automatically generates a hash value of the stored data and sends the hash code to the public blockchain strengthening the overall security of the system.

4.4.4 Blockchain

The public blockchain is a permissionless blockchain, which means that anyone can participate in network governance and transaction origination at any time. To support a number of security features and critical capabilities, the property documentation system is integrated with ethereum, a public blockchain platform. We adopted Ethereum in this systems because it is a decentralized blockchain platform that establishes a peer-to-peer network for securely running and validating application code, known as smart contracts, that allows users to deal with one other without the need for a central authority. It enables the effective operation of smart contracts and apps built on its blockchain, free of fraud, outages, control, or any other external interference. When a user enters or updates any information that causes a smart contract to run, the EVM modifies Ethereum's state to fulfill the requirements of this contract call. The capacity of the EVM to comprehend and execute smart contracts during transactions distinguishes Ethereum from simpler blockchains such as Bitcoin. Eventually, all of the data will be hashed and saved in the public blockchain ledger.

Chapter 5

Data Model

In our data model, the request sent to the blockchain platform (shown in Table 5.2) made up of type and data where TYPE designates the collection of various data kinds that make up a request and type ∈TYPE. Data is the collection of pertinent data and data ∈DATA. The definitions given in (Table 5.2) apply to both TYPE and DATA.

Notations	**Description**
K_{U_f}	Public key of the sender.
$K_{U_f}^{-1}$	Private key of the sender
K_d	Public key of the DApp.
N_i	A fresh nonce.
$\{\}_k$	Encryption operation using a public key K.
$H(M)$	SHA-256 hashing operation of message M.
$[]_{https}$	Communication over HTTPS channel.

Table 5.1: Cryptographic Notations

This is a request and response type data model and the request sent to the blockchain platform (shown in Table 5.2). Also, the response consists of type and data where TYPE designates the collection of various data kinds that make up a request and type ∈TYPE. Data is the collection of pertinent data and data ∈DATA. The definitions given in Table 5.2 apply to both TYPE and DATA.

The queries that users will make such as registration, login, createToken, seacrchToken, tokenDetails, sellToken, buyToken, rentToken, transactionHistory are included in this REQTYPE. For each request made, REQTYPE will contain a REQDATA field, such as regData, loginData, createTokenData, seacrchTokenData, tokenDetailsData, sellTokenData, buyTokenData, rentTokenData, transactionHistoryData. Similar to this, each request will also have a RESPTYPE and RESPDATA. RESPTYPE includes the following functions: regResp, createTokenResp, loginResp, seacrchTokenResp, tokenDetailsResp, sellTokenResp, buyTokenResp, rentTokenResp, transactionHistoryResp. RESPDATA will contain the following fields : regData, loginData, createTokenData, seacrchTokenData, tokenDetailsData, sellTokenData, buyTokenData, rentTokenData, transactionHistoryData. Furthermore, every feature of request data and response data are defined here as what information they will consist of. For example, regisData will consist of userData, h=H(Password)

Req = {reqType, reqData}
Resp = {respType, respData}
REQTYPE = {registration, login, createToken, seacrchToken, tokenDetails, sellToken, buyToken, rentToken, transactionHistory}
REQDATA = {regData, loginData, createTokenData, seacrchTokenData, tokenDetailsData, sellTokenData, buyTokenData, rentTokenData, transactionHistoryData}
regisData = {userData, h}
userData = {Full Name, DoB, NID Number, Present Address, Permanent Address, Phone Number}
loginData = {userId, password, h}
createTokenData = {propertyAddress, propertyImage, propertyRentPrice/propertySellPrice, propertyOwnerPublicKey}
seacrchTokenData = {tokenNumber}
tokenDetailsData = {tokenNumber, propertyAddress, propertyImage, propertyRentPrice/propertySellPrice}
sellTokenData = {tokenNumber}
buyTokenData = {tokenNumber, buyerPublicKey}
rentTokenData = {tokenNumber, renterrPublicKey}
transactionHistoryData = {userPublicKey}
buyerIDData/sellerIDData = {userData}
RESPTYPE = {regResp, createTokenResp, loginResp, seacrchTokenResp, tokenDetailsResp, sellTokenResp, buyTokenResp, rentTokenResp,transactionHistoryResp}
RESPDATA = {resp, K, K^{-1}}

Table 5.2: Data Model

which implies that a registration request must contain a username and the hash of the password. Similarly, we just need the information of userId, password, h for login. Then, userData where we need some personal profile information like Full Name, DoB, NID Number, Present Address, Permanent Address, Phone Number. For propertydata, we need property related information like, tokenNumber, propertyAddress, propertyImage, propertyRentPrice/propertySellPrice. The same entities of propertyData are also used for createTokenData including propertyAddress, propertyImage, propertyRentPrice/propertySellPrice, propertyOwnerPublicKey. Also, for selling, buying and renting property data we need one same entity which is property Id and accordingly buyerId for selling, sellerId for selling and userId for property data.

Algorithm : To interact with the system, an user must register or login himself following the steps presented in Algorithm - 1. To start with, the function for registration (REGISTRATIONFUNC) is executed, when a new user comes in to register himself to the system (line 2). It firstly checks if the user against the given data is already registered or not (line 3). If he is registered already, it denies the request and if not, the user gets regustered and the user information is stired in blockchain (line 4 to 6). Next, if a regustered user wants to login to the system, the LOGINFUNC function is invoked (line 9). In this function, the smart contract matches the given login id and password with the stored user information (line 10). If it matches, the user gets logged in, if not, he gets denied (line 11 to 13).

In this paragraph, the token related functions namely CREATETOKENFUNC (line 16), BUYTOKENFUNC (line 21), SELLTOKENFUNC (line 29), RENTTOKENFUNC (line 34) and LEAVETOKENFUNC (line 40) are described. Starting with the first one, whenever a property owner wants to make his property available in the marketplace, the CREATETOKENFUNC is called. The function automatically generates a unique token id for the property and stores corresponding data to the blockchain (line 17 to 19). Then, the BUYTOKENFUNC works whenever a buyer wants to buy an available property. It (function) checks its (property) availability (line 22), makes unavailable in the marketplace (line 23), records the date (line 24), transfers the amount of price to the owner (line 25) and finally, transfers the ownership from the seller to the buyer (line 26). Next, if any owner wants to sell his property, the SELLTOKENFUNC is executed. Here, it firstly checks whether the user is the real owner or not (line 30). If it passes the condition, the algorithm requests for a new token for the property to display on the marketplace (line 31). However, an user can also rent a property. For this, the system calls for the function, RENTTOKENFUNC and it checks if the property token is rentable (line 35). If so, the system makes the property unavailable on the marketplace for the time it has been rented (line 36) and tranfers the rental amount of price to the owner (line 37). The LEAVETOKENFUNC is executed at the time of leaving the rented property by a renter. If the date of agreement is earlier than the request date, it allows the renter to leave the property (line 41, 42). Otherwise, it denies leaving the property at that time (line 43, 44).

Algorithm 1 : AppartmentMarketPlace

```
1: START
2: function registrationFunc(data)
3:     if User id was stored then
4:         Denied for registration;
5:     else
6:         Store data in Blockchain;
7:     end if
8: end function
9: function loginFunc(data)
10:    if User data matched with stored data then
11:        Login;
12:    else
13:        Denied for Login;
14:    end if
15: end function
16: function createTokenFunc(data)
17:    tokenId := Generate unique token id;
18:    Make available for market-place;
19:    Store data in Blockchain;
20: end function
21: function buyTokenFunc(data)
22:    if data.tokenID is available then
23:        Make unavailable for market-place;
24:        date := Update buying time;
25:        Send money to the owner;
26:        Transfer ownership;
27:    end if
28: end function
29: function sellTokenFunc(data)
30:    if user id is matched with owner address then
31:        Create new token;
32:    end if
33: end function
34: function rentTokenFunc(data)
35:    if data.tokenID is rent-able then
36:        Make unavailable for a time period;
37:        Send money to the owner;
38:    end if
39: end function
40: function leaveTokenFunc(data)
41:    if present date > agreement date then
42:        Leave this token;
43:    else
44:        You can not return token at this moment;
45:    end if
46: end function
47: END
```

Chapter 6

Implementation and Protocol Flow

6.1 Implementation

For our system execution, implementation can be considered as the most significant and crucial part. However, for this phase of our thesis, we have implemented the user interface which is DApp for our system and integrated it with IPFS.

Used Technologies: In the development, we have used html, tailwind which is a CSS framework and react.js for front-end and javascript, Solidity for backend [24]. Moreover, we have used ERC721 which is a standard for representing ownership of non-fungible tokens, that is, where each token is unique, Hardhat for development environment and Goreli which is a Proof-of-Stake (PoS) testnet designed to simulate the behaviour of the Ethereum mainnet and Alchemy that offers a powerful blockchain or web3 development platform. Below, we are presenting and explaining a glimpse of it.

This is our home page (shown in Figure 6.1) where users will be initially directed to and the users can view all the available property. If they want to get more details or interact with any particular property they will have to register for it.

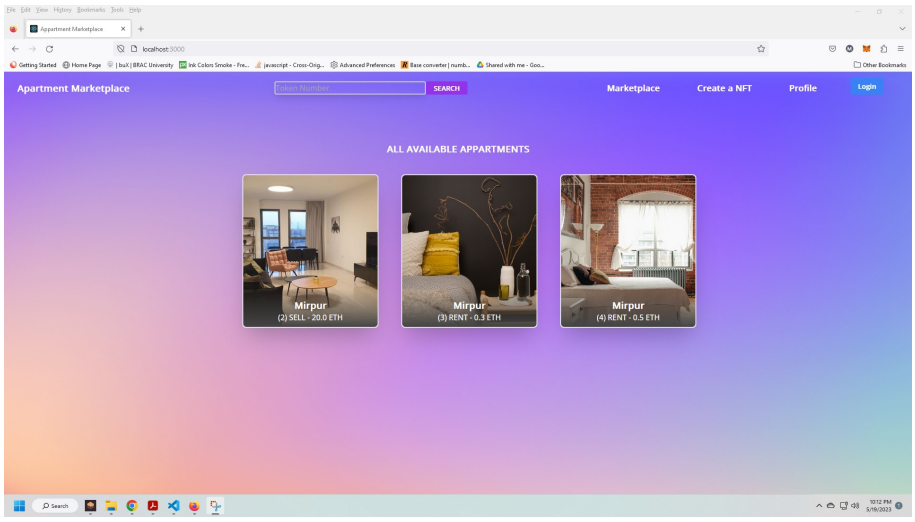


Figure 6.1: Home Page

In Figure 6.2 and Figure 6.3, we are showcasing our Registration and login interface.

Here, users must register with their valid information and only then they will be able to login to the website.

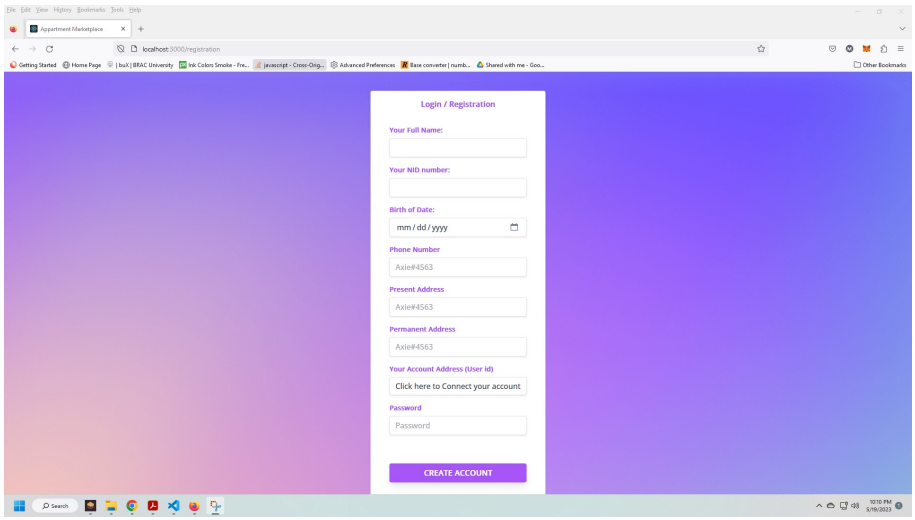


Figure 6.2: Registration Page

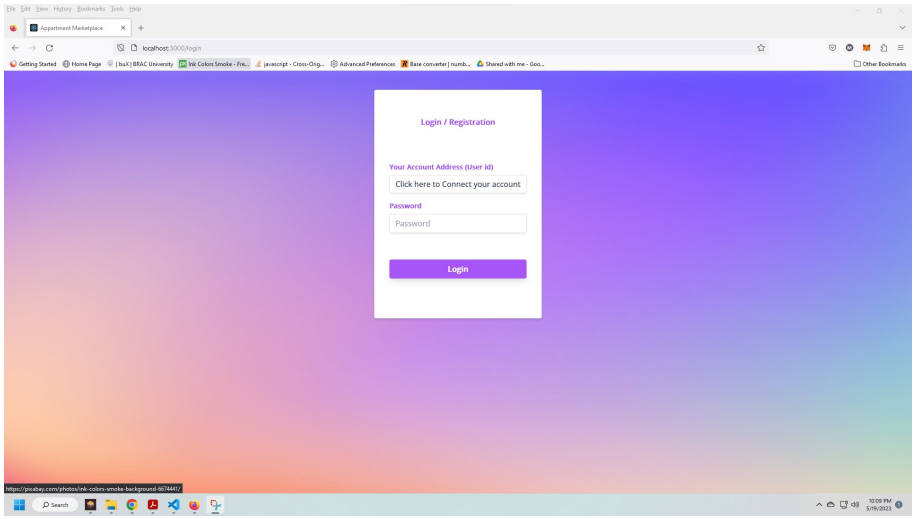


Figure 6.3: Login Page

Next, in Figure 6.4, profile details and all the property details are displayed in two separate sections. In the first and second section, users' own property and rented property details are displayed respectively. Also, there is a button that takes user to the transaction history page.

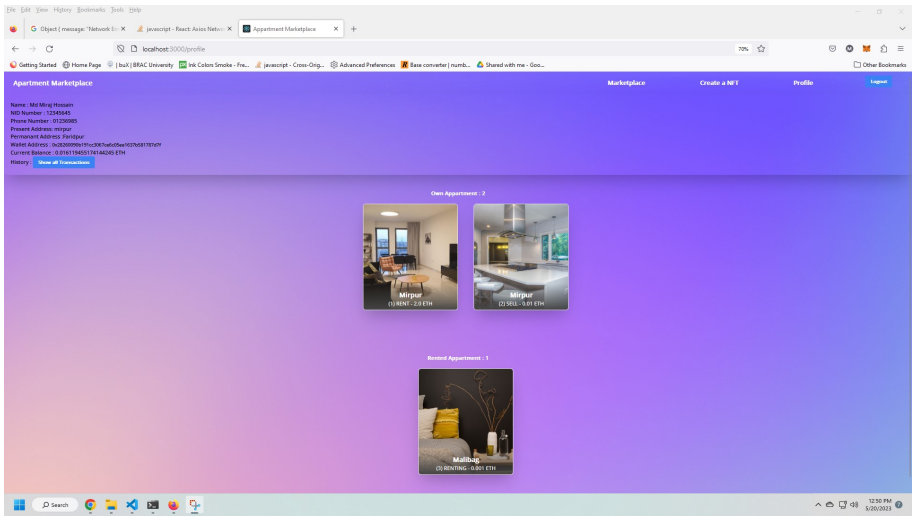


Figure 6.4: User Profile Page

Next, in Figure 6.5, we are showcasing Create Token user-interface. Here, users must register with their valid information and provide valid property details to be able to create property token.

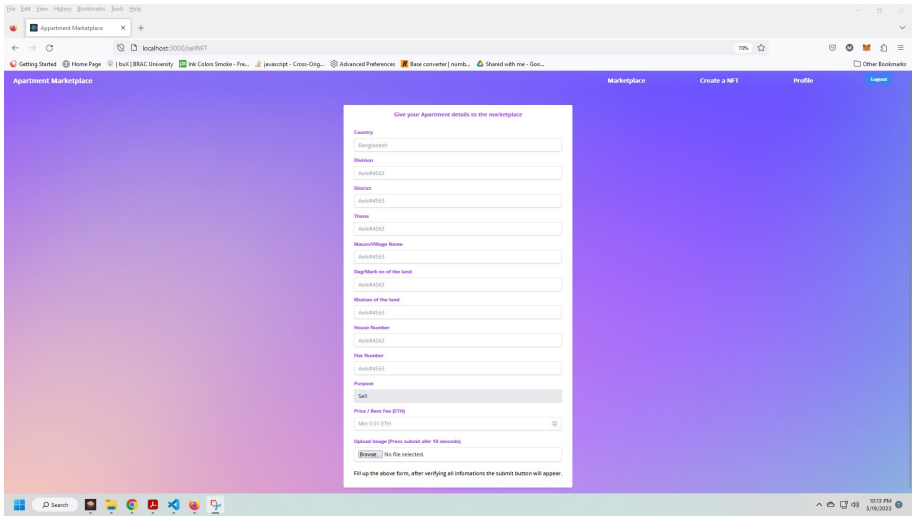


Figure 6.5: Token creation Page

In Figure 6.6, Figure 6.7, Figure 6.8 and Figure 6.9, we are showcasing the property details page where users can buy, sell, rent and leave according to the agreement and their preference.

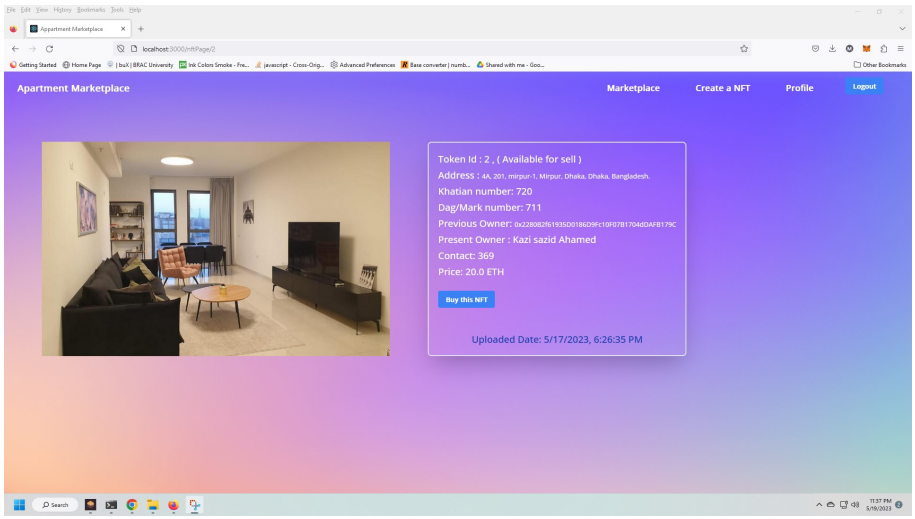


Figure 6.6: Buy Token Page

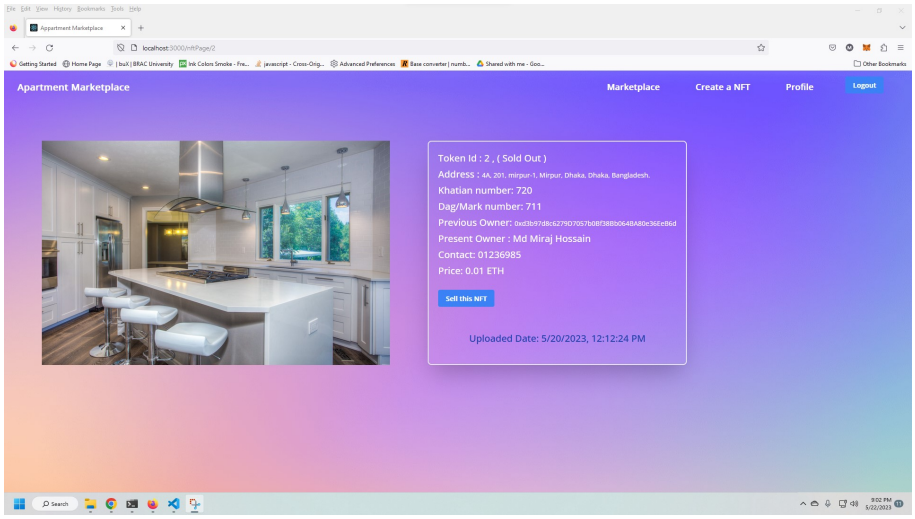


Figure 6.7: Sell Token Page

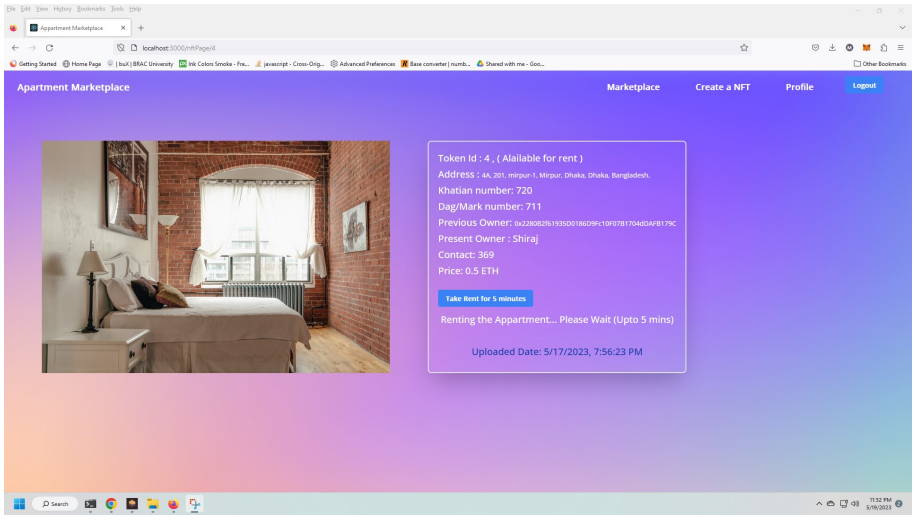


Figure 6.8: Rent Token Page

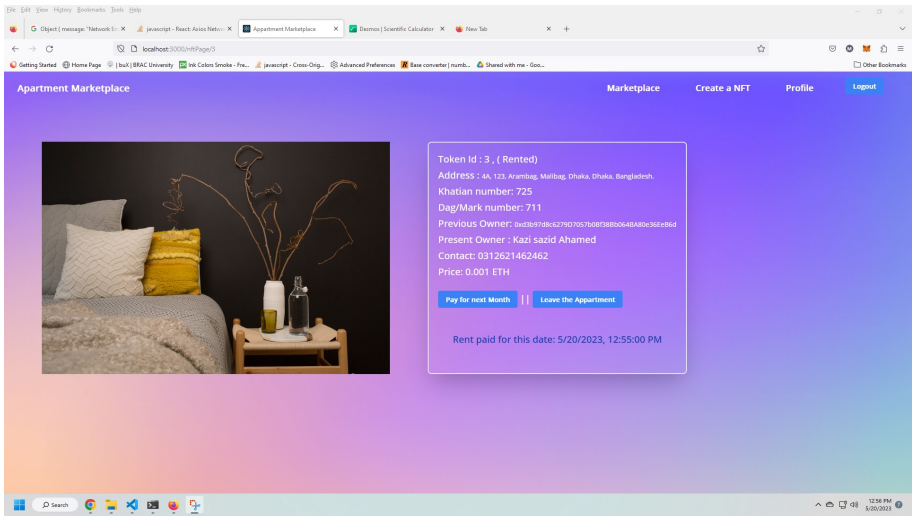


Figure 6.9: Leave Token Page

6.2 Protocol Flow

Protocol flow: In this part, we present the protocol flow involving various components of our system's design. We have divided the entire flow into three main parts: 1) User registration and login, 2) Property token creation and 3) Buying, selling, renting or leaving token.

6.2.1 User registration and login

A new user must register in order to interact with our DApp following the registration protocol. The protocol flow is provided in Table 6.1 and illustrated in Figure 6.10. In the following points, we discuss the flow in brief.

M_0	$User \rightarrow DApp:$	$[N1, \{userInfo\}K_{U_f}^{-1}]_{https}$
M_1	$DApp \rightarrow API:$	$[N2, req]_{https}$
M_2	$API \rightarrow DApp:$	$[N2, resp]_{https}$
M_3	$DApp \rightarrow IPFS:$	$N3, string$
M_4	$IPFS \rightarrow DApp:$	$N3, \{resp\}K$
M_5	$DApp \rightarrow Blockchain:$	$N4, H(string)$
M_6	$Blockchain \rightarrow Dapp:$	$N4, TRUE$
M_7	$DApp \rightarrow User:$	$[N1, \{resp\}K_d]_{https}$

Table 6.1: Registration protocol

- At first, the user gets a registration form (Figure 6.2) with some information fields to be filled up such as name, NID number, mobile number, date of birth, userID and password (denoted with M0 in Table 6.1). The userID here is mainly the account address which is public key and unique for every individual user. The password is hashed using the SHA-256 algorithm.
- The DApp then sends the NID and birth date to a third party API to verify the user (denoted with M1 in Table 6.1).

- At reply, the API sends the response signal whether the user gets verified or not (denoted with M2 in Table 6.1).
- In the next step, the less sensitive data except userID and hashed password is sent to IPFS blockchain platform from DApp (denoted with M3 in Table 6.1) to store the data and it (IPFS) sends the hash value of storing address back to the DApp (denoted with M4 in Table 6.1).
- Then, the DApp sends the hashed address, userID and hashed password to the blockchain to store (denoted with M5 in Table 6.1) and the blockchain stores it .
- After storing the data effectively, a TRUE signal is sent back to the DApp from blockchain (denoted with M6 in Table 6.1) and consequently, DApp displays a confirmation message to the user stating he (the user) is registered to the system successfully (denoted with M7 in Table 6.1).

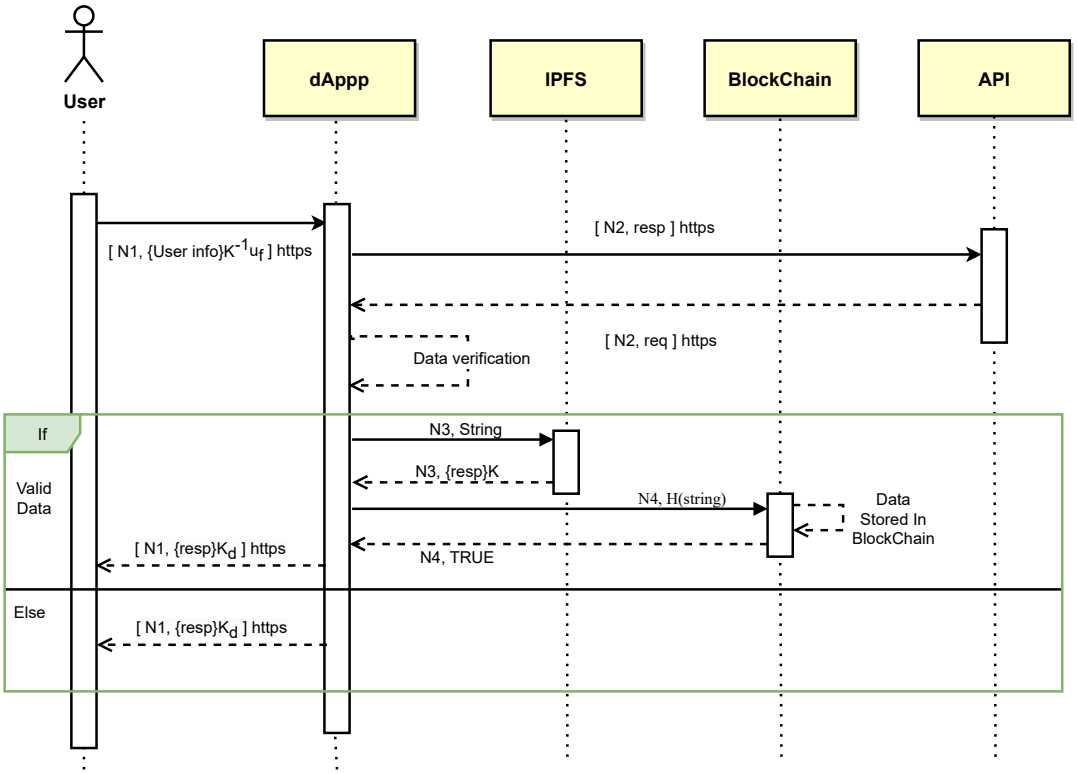


Figure 6.10: Registration

Before using the service, each user must log (Figure 6.3) in to the system. Similar to the registration protocol, the login protocol requires the user to provide their username and password through their browser. This time. the login function is invoked. The underlying algorithm matches the credentials given by the user with the initially stored data in blockchain and returns TRUE/FALSE based on its matching outcome.

6.2.2 Property token creation

In the present section, we discuss how an individual token is created against a property in our system architecture. This protocol is invoked whenever a property owner leaves his property to sell in the marketplace. The flow is presented in Table 6.2 and demonstrated in Figure 6.11. A brief idea of this protocol is as follows.

M_0	$User \rightarrow DApp:$	$[N1, \{tokenInfo\}K_{U_f}^{-1}]_{https}$
M_1	$DApp \rightarrow API:$	$[N2, req]_{https}$
M_2	$API \rightarrow DApp:$	$[N2, resp]_{https}$
M_3	$DApp \rightarrow IPFS:$	$N3, Image$
M_4	$IPFS \rightarrow DApp:$	$N3, \{resp\}K$
M_5	$DApp \rightarrow IPFS:$	$N4, string$
M_6	$IPFS \rightarrow DApp:$	$N4, \{resp\}K$
M_7	$DApp \rightarrow Blockchain:$	$N5, H(string)$
M_8	$Blockchain \rightarrow DApp:$	$N5, TRUE$
M_9	$DApp \rightarrow User:$	$[N1, \{resp\}K_d]_{https}$

Table 6.2: Token Creation/Add property protocol

- Starting with, the owner submits his property information to the user interface (Figure 6.5) of the DApp (denoted with M0 in table 6.2).
- Next, the DApp sends the given data to the 3rd party application (which is now an ongoing project as well) to verify the property information through API (denoted with M1 in table 6.2). If it is verified successfully, the application will reply back a signal with positive response to the DApp (denoted with M2 in table 6.2). The property is eligible now to get a unique token id once it is verified correctly.
- Now, to store the property information, DApp sends the property credentials to the IPFS database in two consequent steps. Firstly, DApp sends its picture (denoted with M3 in table 6.2) and IPFS sends back a hash value in response (denoted with M4 in table 6.2). At the following step, the DApp again sends the other information along with the returned hash value of the image to IPFS (denoted with M5 in table 6.2) and this time, IPFS returns a bigger hash value (denoted with M6 in table 6.2).
- At this point, the DApp sends a token creation request to the blockchain (denoted with M7 in table 6.2) with the bigger hash value sent by IPFS. Getting this, the underlying algorithm generates a random unique number as a token against the particular property as well as checks if it is available for a new token or not.
- If the number is available, it is registered as the token id to the property. Then, the assigned token id along with the hashed value returned from IPFS is stored in the blockchain.
- After that, a TRUE signal is sent from blockchain to DApp denoting a successful token creation and the DApp shows a confirmation message to the user (denoted with M8 and M9 in table 6.2).

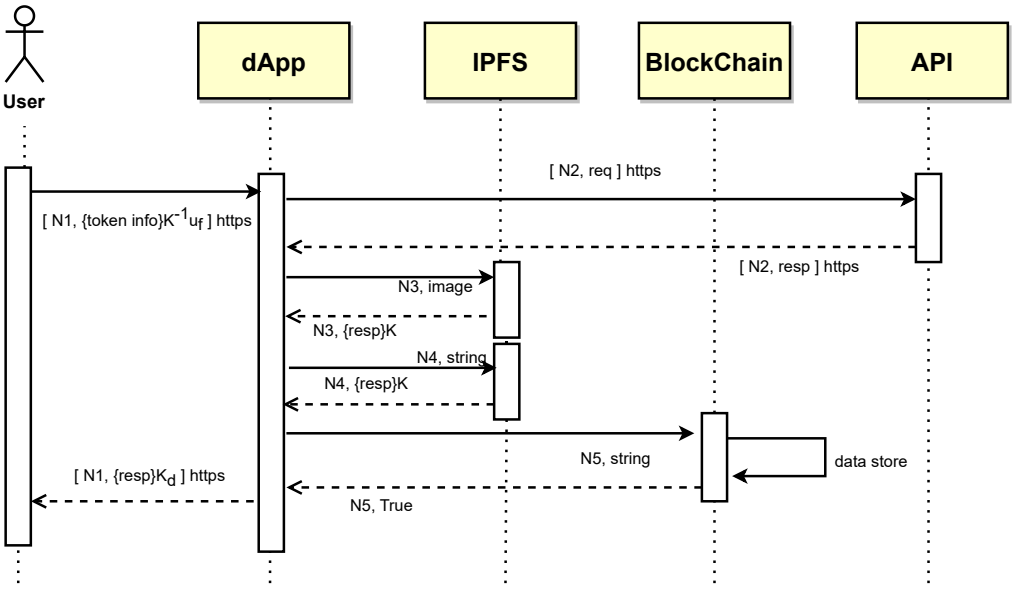


Figure 6.11: Token Creation

6.2.3 Buying, selling, renting or leaving token

In this section, we describe how a token is bought, sold, rented or left by a user in our underlying system. In our platform, a token is actually a property. However, there are four individual working functions for the aforesaid four individual actions to be performed but the protocol is the same for all of them. To make the process more clear to be understood, this flow is presented in Table 6.3 and Figure 6.12. Here, a concise description of this protocol flow is given below.

M_0	$User \rightarrow DApp:$	$[N1, \{string\}K_{U_f}^{-1}\ ]_{https}$
M_1	$DApp \rightarrow Blockchain:$	$N2, H(string)$
M_2	$Blockchain \rightarrow DApp:$	$N2, TRUE$
M_3	$DApp \rightarrow User:$	$[N1, \{resp\}K_d\ ]_{https}$

Table 6.3: Buy/Sell/Rent/Leave protocol

BUY

- To start with, if anyone wants to buy a property (denoted with M0 in Table 6.3), the buyer needs to click the "Buy this NFT" option in the DApp (corresponding user interface is shown in Figure 6.6). The DApp accordingly sends the request to the blockchain 6.3 and the blockchain checks its availability and price.
- If it (blockchain) finds it (property) available, the total amount of its (property) price is transferred to the seller's wallet from the buyer's wallet through blockchain transaction and immediately, the ownership is shifted from seller to buyer. Also, it makes the property unavailable for buying for the time being and is removed from the marketplace .

- Finally, the blockchain returns a TRUE signal to DApp (denoted with M2 in Table 6.3) and it (DApp) through its user-interface displays a confirmation message to the user (denoted with M3 in Table 6.3).

SELL

- Next, if there is invoked a sell request from any user (denoted with M0 in Table 6.3), the particular sell function is invoked. Here again, after getting the sell request from DApp (denoted with M1 in Table 6.3), the blockchain firstly checks the property address and whether its availability is FALSE.
- If the conditions are satisfied, it calls the responsible function for creating the token (described in the second protocol flow). After that, another unique token is assigned to the property and it is up for sale to the marketplace.

RENT

- An individual function for making a rent of a property is called whenever any user hits the rent option on the marketplace (denoted with M0 in Table 6.3, corresponding user interface is shown in Figure 6.8. To proceed, the DApp sends a rent request to the blockchain (denoted with M1 in Table
- The underlying algorithm then checks whether it (property) is available for renting or not as well as its (property) price. Then, the property is made unavailable for renting once the above-cited conditions are met properly.
- After that, the rental price is automatically moved to the property owner from the renter. Finally, the user gets an approval message from the DApp as soon as the DApp gets a TRUE signal from the blockchain (denoted with M2 and M3 in Table 6.3).

LEAVE

- The function responsible for leaving a rented property is executed once any renter wants to leave the house or property (corresponding user interface is shown in Figure 6.9). Once the function is invoked (denoted with M0 in Table 6.3), it will send a leave token request to the blockchain (denoted with M1 in Table 6.3).
- Then, it internally checks the address and the rental due data. If either one or both the address and due date is not correct it returns a FALSE signal from the blockchain with a negative message to the user.
- If the address and rental due date is correct and satisfies all the requirements then the DApp gets a TRUE signal from blockchain (denoted with M2 in Table 6.3). After getting the TRUE signal from the blockchain, DApp returns a response back to the user (denoted with M3 in Table 6.3).

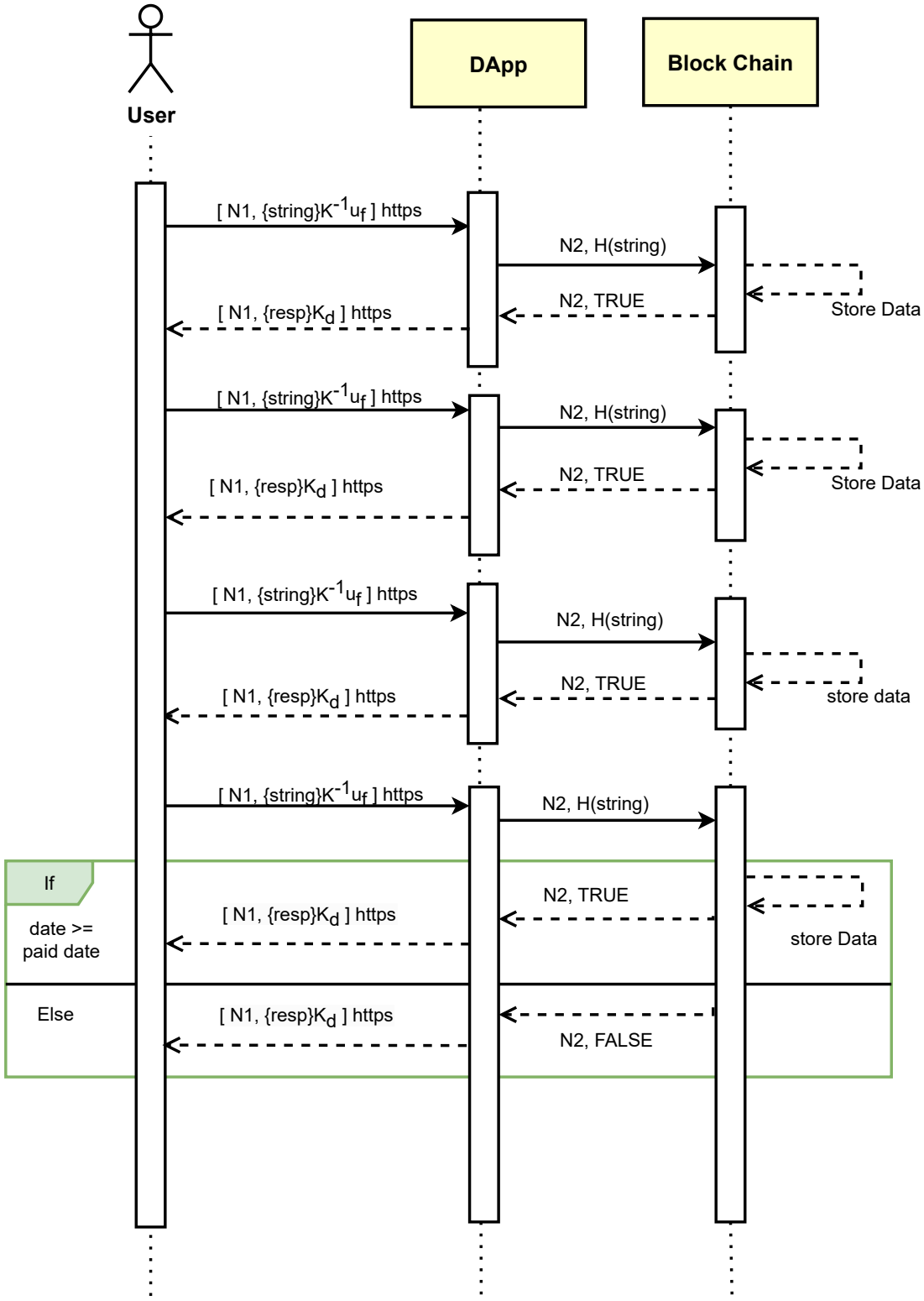


Figure 6.12: Buy-Sell-Rent

Chapter 7

Analysis and Discussion

7.1 Functional Requirement Analysis

Our proposed system meets all the functional and non-functional requirements stated earlier. In our system users will be registered through NID verification ensuring each profile contains valid information and users will have their unique user ID. Only registered users can register their property for selling or renting purpose after giving valid information and the system will showcase those properties in the marketplace as available. Then interested users can buy or rent them from the marketplace which satisfies functional requirements FR1 and FR2 stated earlier. Furthermore, these properties will be tokenized and will have a unique tokenID for each property. Users will buy or rent their property directly from the owner with a peer to peer transaction. Moreover, this system is integrated with the decentralized blockchain platform ensuring the transparency, immutability and trustworthiness as well as satisfying the functional requirements FR3, FR4, FR5 and FR6.

7.2 Security Requirement Analysis

This system is implemented with NID verification as the strong authentication system which satisfies the security requirement SR1. As mentioned earlier, being integrated with the blockchain ensures the data integrity by keeping it immutable and distributed. It also uses an IPFS distributed database and satisfies the security requirements SR2, SR3 and SR5. The system encrypts data during transmission and storage hence satisfies security requirement SR4.

7.3 Research Objective Analysis

During the time of pre-thesis 1, we have set some research objectives (section 1.3 of chapter 1) to be achieved throughout our whole thesis development. In this section, we are going to highlight how we have tried to accomplish those objectives through different phases of our development process.

- In chapter 2 named Background, we have stated detailed descriptions of Blockchain, Cryptocurrency, Ethereum, Tokenization and Property Tokenization. To do this, we have come through quite a clear concept of each of them; particularly

how they work. Thus, we have fulfilled the very first of our research objectives (RO-1).

- We have studied some research papers related to our own proposal gathering the idea about the previously done developments in this field. Besides, we have found out and learned about some related existing platforms too. Thereafter, in chapter 3 named Related Work, we have discussed these learnings and findings and in this way, we have achieved the second objective of our thesis (RO-2).

- We have faced some identical challenges too while implementing our proposal. For instance, operating a blockchain based system which requires the use of cryptocurrency in a country like Bangladesh (region specific challenge), the user or NID verification, property verification etc. To solve these challenges, we are using 3rd party API applications and for region based problems we can say that the experts of this field are already working on mitigating this shortcoming.

- In section 4.3 named Requirement Analysis of chapter 4 of this paper, there is a thorough discussion on the major three types of requirements of our system. We have talked about functional requirements, security requirements and privacy requirements respectively. In this manner, the fourth objective (RO-4) has been met well.

- Our designed architecture consists of three main parts named DApp, IPFS and Public Blockchain which work together to make the system work rationally. We have explained it in section 4.4 of chapter 4 along with a pictorial representation (Figure 4.1. Besides, in section 6.2 of chapter 6 named Protocol Flow, there has been discussion about three complete protocol flows such as User registration and login (sub-section 6.2.1), Property token creation (sub-section 6.2.2) and Buying, selling, renting or leaving protocol (sub-section 6.2.3) together with their respective protocol flow tables Table 6.1, 6.2 and 6.3 and diagrams (Figure 6.10, 6.11 and 6.12). Thus, we have tried to accomplish the fifth research objective, RO-5.

- In section 6.1 of chapter 6, we have explained a step by step implementation of our development process. In such wise, we have attempted to carry out our last objective stated in RO-6.

7.4 Cost Analysis

Cost Analysis: All interface deployment and transaction expenses are shown in Table 7.1 below. The entire transaction cost may cause concern due to the change in ether's price. This is due to the unpredictability of the price of popular cryptocurrencies like bitcoin and ether. The introduction of a private blockchain system,

where the cost of mining may be decreased or eliminated, can easily resolve this issue. A good replacement for that will be the Hyperledger Fabric.

Gas cost in USD on March 17, 2023.

Category	Gas Cost (ETH)	Dollar (USD)	BDT(TAKA)
Contract Deploy	0.0597	107.72	11563.52
Registration	0.000235417999998976	0.42	45.09
Token Creation	0.000435874000011264	0.79	84.80
Buy Token	0.00022198	0.40	42.94
Sell Token	0.000416236000002048	0.75	80.51
Rent Token	0.000162284	0.29	31.13
Return Token	0.000123609999998976	0.22	23.62

Table 7.1: Cost Analysis

Following the Table 7.1, we summarize the system's evaluation of function in relation to the gas costs spent for various system operations. It costs 0.0597 ether to deploy because we have a smart contract that has all the functionality. When the system is initialized, this cost is only charged once. It is the one that the system spends the most money on. The other frequently used functions just need a few amount of ether. As the gas cost is relatively low, it denotes a lesser level of code complexity, which relates to high-performance stability.

The bar chart makes the anticipated gas cost easier to understand (Figure 7.1). Gas prices are shown on the x-axis in ether, and their related function names are shown on the y-axis. It is unambiguous that contract deployments use the most gas compared to other function. It should be highlighted that the current gas cost complications can be eliminated if we use an Ethereum consortium blockchain. This is because the gas price can be limited or eliminated entirely in a consortium blockchain; as a result, it is not a concern.

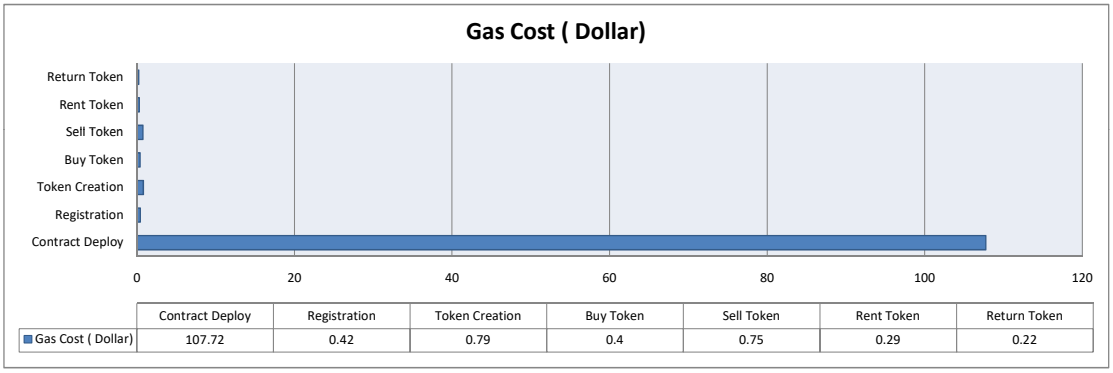


Figure 7.1: Gas Cost

7.5 Comparison

Though both the traditional system and blockchain based system intends to reach the same goal but there are plenty of differences in their way of reaching the goal. We are illustrating some of them below:

Category	**Blockchain App**	**Traditional System**
1.Transparency and Security	Transparency is provided by the blockchain, which delivers a decentralised, unchangeable ledger that records all transactions and property information. By doing so, confidence is increased and the danger of fraud is decreased because the information is protected from tampering and is available to all authorised parties.	In a traditional system, information is typically centralised and managed by middlemen, creating information asymmetry and potential weaknesses. The integrity and reputation of these intermediaries are essential for building trust.
2.Smart Contracts	Smart contracts are self-executing contracts that automatically enforce predetermined conditions when particular criteria are satisfied. These contracts make it possible to automate procedures like property transfers and rent collection which eliminates the need of middlemen and lowers the transaction costs.	Conventional contracts frequently call for manual intervention which causes delays, mistakes made by humans, and additional expenditures. They might need middlemen to help enforce the terms like attorneys or agents.

3.Global Accessibility	Blockchain technology allows for global accessibility to real estate listings and transactions. Anyone with access to the internet can participate, broadening the audience and pool of potential buyers or tenants. It makes cross-border transactions easier and offers chances for foreign investors.	Potential tenants or buyers outside of a certain region may find it difficult to participate in traditional systems because they frequently have geographical restrictions. Legal regulations and linguistic limitations may add extra complexity to international transactions.
4.Cost Reduction	Blockchain apps can drastically lower transaction costs related to buying, selling and renting properties by eliminating middlemen, streamlining procedures and automating jobs. Smart contracts do away with the need for middlemen which lowers costs and the likelihood of disputes.	Traditional methods have a number of expenditures including agent commissions, legal fees and administrative expenses. These costs may accumulate and raise the total price of purchasing, selling or leasing a property. While apps for renting and selling on the blockchain have many benefits, it's crucial to remember that integration with current systems and regulations as well as general acceptance may take some time. However, blockchain technology is a potential game-changer in the real estate sector due to the potential for improved transparency, efficiency and cost savings.
5.Speed and Efficiency	Blockchain-based apps for renting and selling property automate procedures, reduce manual intervention and eliminate paperwork. The ability to complete property listings, verification, payments and documentation more quickly enables more efficient transactions.	The conventional system entails laborious procedures such as paper-based documentation, manual verifications and collaboration between numerous parties. These procedures may slow down transactional speed overall and result in delays.

The concept and idea underlying our system is completely distinctive in Bangladesh and differs even from comparable existing platforms used elsewhere in the world. If we talk about the perspective of Bangladesh, there do exist some online platforms offering property renting or selling services though, but there are no decentralised and transparent ones of this kind. So, we are working on introducing such an essential system to the Bangladeshi people so that they can get rid of everyday hassles and deceptions they have to go through in these fields. Not only this, there are some different features from the international platforms too. They are pointed below accordingly.

- We are offering both the trading and renting services alongside and there is no such kind of platform offering these two services in one place.
- Our platform is a whole decentralised one as we are using blockchain for storing sensitive data and IPFS which is also a blockchain decentralised platform to store the less sensitive data. We have no central database and at the same time, it is also a cost efficient one from the perspective of blockchain costing. On the other hand, the relatively existing platforms maintain personal central database/s to some extent.
- We are still working on room wise tokenization which will be able to meet demand of each kind of seller, buyer and renter.

7.6 Advantages

This system offers a bunch of advantages. Here, we are going to highlight some of them:

- This is a very primary work to showcase how the blockchain can be leveraged to make the property renting or selling system decentralised and transparent.
- In this system, we are incorporating smart-contract technology to avoid typical paperwork and mitigate any kind of agreemental issues between two parties.
- We are using NID verification of the users and providing unique token ids to each individual property to reduce fraudulence in the system.
- We are assuring peer to peer transactions to avoid any unwanted incident due to the broker parties in this field.

7.7 Limitations and Future Works

We have observed some limitations in our system and hereafter, we have further schemes to overcome these shortcomings. To start with, there are still countries like Bangladesh in which crypto-currency and crypto-transaction are not legalised but it is very evident that it will be legalised in the very near future as the modern world is already executing the manner. To proceed with, we also do not have any property verification API right now but will have one in no time as this is an ongoing project as well. When we will be able to add this API, this system will become

more trustworthy and handy for common people. Moreover, in our system, we are using public blockchain for the time being as it is a primary implemention of our idea using blockchain technology. However, public blockchain is more costly than private blockchain and in future, we are planning to move to private blockchain to store the data which will make the system more cost efficient.

In addition to the above mentioned points, we have also several plans implementing some more other features concerning our system. Regarding this, we have an intention adding the idea of micro-property concept to our platform meaning that a property will be divided into its micro components. To clarify, we will keep an option of buying a single room or two or multiple of an entire house according to the demand of buyers. To do so, we will tokenize an entire house in accordance with its rooms denoting that each room will have a different token id. Here, at the time of leaving the property for the marketplace, the owner will see the option of how he wants to tokenize it; room wise or as a whole. We believe that it will add a distinguished level to our system which will be immensely useful for all; both the buyers and sellers. Furthermore, we will try to add a feature of face recognition along with NID verification at the time of registration to ensure an extra security of the system. Besides, some IoT devices may be implemented physically in the rentable houses that will work together with the virtual smart contracts keeping the rental agreements rigid in physical level too.

Chapter 8

Conclusion

To conclude, home is one of the most crucial human needs that is intimately related to our existence. People are moving from one capital to another, or even from one country to another, in an effort to improve their quality of life, their chances of earning more money, or both. Therefore, renting, selling and purchasing homes is constantly necessary, which comes with a number of obstacles. Here, we are conducting our research to look for a workable solution to lessen these issues and make it accessible to everyone throughout the world. We have finished gathering background data, researching relevant literature, and composing our research proposal in the pre-thesis 1. Following that in pre-thesis 2, we did a requirement analysis based on a thorough threat model to reduce any potential threats to our system. Then we gave a quick description of our architecture plan. Additionally, we included a brief explanation and a draft of our data model. In addition, we began implementing it and added a sneak preview of it. Finally, to give our research a flawless ending, we wrapped up our protocol flow, algorithm, remaining implementation, discussion and analysis in the final thesis period. Lastly, we do hope and believe that our research will definitely leave a lasting impression.

Bibliography

[1] C. M. R. P. Limited, *Global blockchain technology market size worth $69 billion by 2030 at a 68% cagr check blockchain industry share, growth, trends, value amp; analysis: Custom market insights*, Aug. 2022. [Online]. Available: https://www.globenewswire.com/en/news-release/2022/08/25/2504745/0/en/Global-Blockchain-Technology-Market-Size-Worth-69-Billion-by-2030-at-a-68-CAGR-Check-Blockchain-Industry-Share-Growth-Trends-Value-Analysis-Custom-Market-Insights.html.

[2] J. Falcon, *Fraudulent rental applications have spiked during pandemic*, May 2020. [Online]. Available: https://www.housingwire.com/articles/fraudulent-rental-applications-have-spiked-during-pandemic/.

[3] Admin, *The risks of accepting cash payments for rent*, Oct. 2022. [Online]. Available: https://innago.com/risks-cash-payments/.

[4] A. Ann O'Connell, *Can our landlord evict us to move the landlord's family member in?* Oct. 2022. [Online]. Available: https://www.nolo.com/legal-encyclopedia/question-evict-landlord-family-member-28362.html.

[5] S. F. Kabir, *Seeking shelter in the big city – issues between landlord and tenant in bangladesh*, Oct. 2012. [Online]. Available: https://www.vertexchambers.com/blawg-list/seeking-shelter-in-the-big-city-issues-between-landlord-and-tenant-in-bangladesh-october-2012-issue-1/?fbclid=IwAR2FBwew5VHxL5_ijRFuxE_J_pyvnsufKYz7wvBfM6bnAo1eGO4iIFei9Vs.

[6] Admin, *Cryptocurrency trading not allowed at all : Bangladesh bank*, Oct. 2022. [Online]. Available: https://www.thedailystar.net/business/news/cryptocurrency-trading-not-allowed-all-bangladesh-bank-2140141.

[7] *What is blockchain technology - ibm blockchain*, Oct. 2022. [Online]. Available: https://www.ibm.com/topics/blockchain.

[8] *What is proof of work pow() in blockchain?* Sep. 2022. [Online]. Available: https://www.investopedia.com/terms/p/proof-work.asp.

[9] *What does proof-of-stake (pos) mean in crypto?* Sep. 2022. [Online]. Available: https://www.investopedia.com/terms/p/proof-stake-pos.asp.

[10] *What is cryptocurrency and how does it work?* Sep. 2022. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency.

[11] *All cryptocurrencies*, Sep. 2022. [Online]. Available: https://coinmarketcap.com/all/views/all/.

[12] *What is bitcoin and how does it work?* Sep. 2022. [Online]. Available: https://www.forbes.com/advisor/investing/cryptocurrency/what-is-bitcoin/.

[13] *What is ethereum? how does it work?* Sep. 2022. [Online]. Available: https://www.forbes.com/advisor/investing/cryptocurrency/what-is-ethereum-ether/.

[14] *What is tether? how does it work?* Sep. 2022. [Online]. Available: https://www.forbes.com/advisor/investing/cryptocurrency/what-is-ethereum-ether/.

[15] *Binance.us review 2023*, Sep. 2022. [Online]. Available: https://www.forbes.com/advisor/investing/cryptocurrency/binance-us-review/.

[16] *Ethereum*, Sep. 2022. [Online]. Available: https://en.wikipedia.org/wiki/Ethereum.

[17] *What are smart contracts on the blockchain and how they work*, Sep. 2022. [Online]. Available: https://www.investopedia.com/terms/s/smart-contracts.asp.

[18] *Tokenization*, Nov. 2022. [Online]. Available: https://id4d.worldbank.org/guide/tokenization.

[19] *Coingape media on binance feed: Tokenization: What is it and how does it work?* Nov. 2022. [Online]. Available: https://www.binance.com/en/feed/post/158446.

[20] Admin, *Empirical evidence on the ownership and liquidity of real estate tokens*, Oct. 2022. [Online]. Available: https://innago.com/risks-cash-payments/.

[21] Admin, *Tokenization—the future of real estate investment?* Oct. 2022. [Online]. Available: https://innago.com/risks-cash-payments/.

[22] J. Smith, M. Vora, H. Benedetti, K. Yoshida, and Z. Vogel, *Tokenized securities and commercial real estate*, Aug. 2019. [Online]. Available: https://ssrn.com/abstract=3438286.

[23] Node.js. [Online]. Available: https://nodejs.org/en.

[24] *Node.js web application framework*. [Online]. Available: https://expressjs.com/.