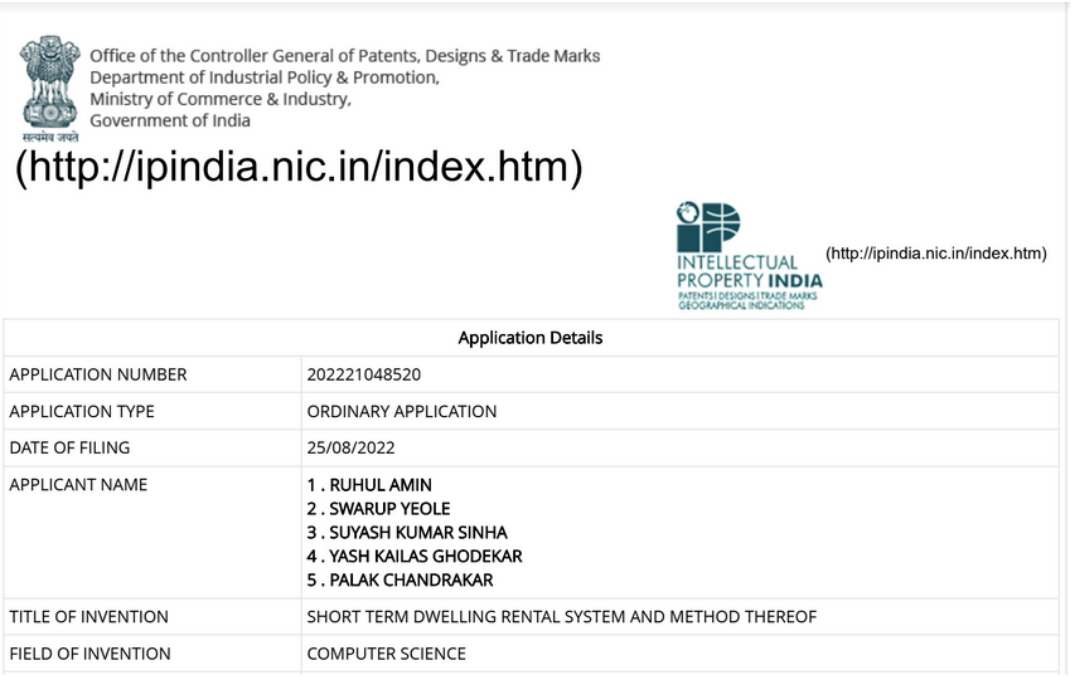
PROJECT REPORT

SHORT TERM DWELLING AND METHOD



Office of the Controller General of Patents, Designs & Trade Marks
Department of Industrial Policy & Promotion,
Ministry of Commerce & Industry,
Government of India
(http://ipindia.nic.in/index.htm)

INTELLECTUAL PROPERTY INDIA (http://ipindia.nic.in/index.htm)

Application Details	
APPLICATION NUMBER	202221048520
APPLICATION TYPE	ORDINARY APPLICATION
DATE OF FILING	25/08/2022
APPLICANT NAME	1 . RUHUL AMIN 2 . SWARUP YEOLE 3 . SUYASH KUMAR SINHA 4 . YASH KAILAS GHODEKAR 5 . PALAK CHANDRAKAR
TITLE OF INVENTION	SHORT TERM DWELLING RENTAL SYSTEM AND METHOD THEREOF
FIELD OF INVENTION	COMPUTER SCIENCE

ABSTRACT

Over the years, the hospitality industry has been revolutionized. Before 2008, travellers would have likely booked a hotel or hostel for their trip to another town. But now a person having a home or even a room can rent it out to people. The main idea is to find a way for local people to make some extra money renting out their spare homes or rooms to people visiting the area.
Many centralised platforms like Airbnb provide short-term renting, and several others offer long-term renting, such as MagicBricks, NoBroker, etc. The dominance rests atop exploitation of the hosts and guests that are doing the sharing and creating the value. The guests pay too much, and the hosts are paid too little. Users' private data like location could be compromised due to the centralisation of the data. Brokerage and various hidden fees are charged for using the platform.

Offer a Decentralized housing rental system for short-term rentals. Achieve peer-to-peer sharing of listings information in an intermediary-free manner. Convert traditional lease methods into smart contracts. Improve the efficiency of the lease process. Store all the information related to the contract in a secure blockchain system

Table of Contents

List of All Figures

CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION

We're bound with technology when all we want is simple functionality. With the present technological paradigm shift, it is more important than ever to embrace and understand the potential of technology. The rental sector stays vigilant in the face of change, adopting a new method that makes it a lot easier to manage rental properties. As a result, there is a need to design a rental house system that can simplify work using cutting-edge technology, allowing users to be more efficient and productive.

Currently, the market offers a variety of solutions/platforms for long-term rentals, but there are few and pricey possibilities for short-term rentals of a home. All current short-term rental solutions are based on a centralized method in which a single association collects all user data and distributes it to other users. Unfortunately, hackers can access all user data in order to obtain private information such as users' addresses and contact information, resulting in a privacy issue. This type of data breach has previously occurred, resulting in significant private information leaks. Another concern is that these companies act as middlemen, charging exorbitant fees to individuals who use their services, resulting in overpriced rental apartments.

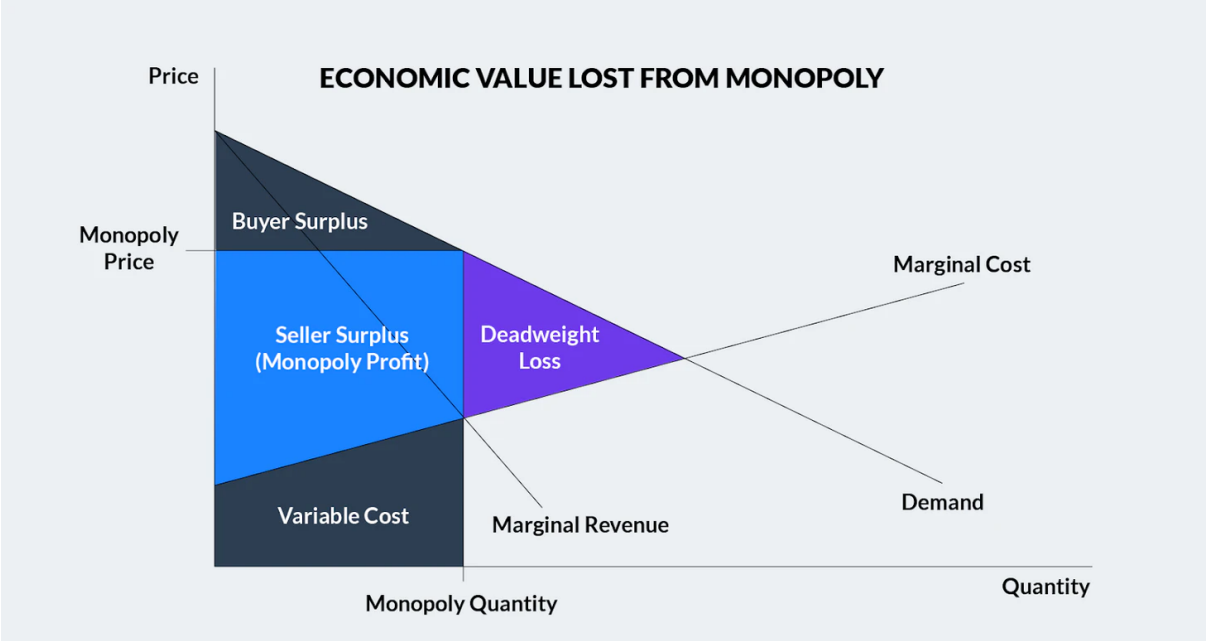


Fig. 1.1 Title

All of the above-mentioned problems can be solved by decentralization of the platform providing these services which is the main objective of our invention. This research project focuses on managing rental houses for low income, medium and high-income households or what is commonly known as affordable housing. The term "affordable" refers to a person's capacity to pay for a specific product or service because their income allows them to do so. Although the term "affordable housing" is frequently used to refer to rental property that is within the financial reach of those in lower-income areas of a geographic area, the notion applies to both middle and high-income individuals.

Due to decentralization and the use of blockchain for transactions, the transaction records are immutable, and user data is secure since no intermediaries are involved in the transaction. The removal of intermediaries also reduces the intermediary fees of the rental property resulting in lower rent prices. Even though prices are lower for the consumer, it does not mean that the owner is getting paid less compared to centralized systems since it involves intermediary fees, which are negligible in a decentralized system. Thus, this system benefits both owner and tenant. Another advantage of a Decentralized system is that all the transactions are recorded digitally and are paperless, thus reducing the environmental impact.

CHAPTER 2

LITERATURE REVIEW

2.1 Smart Contract for Lease Agreements using Blockchain Technology, Macha Shanker

This paper aims to present the Blockchain and smart contract for a specific domain that deals with real estate to solve issues like avoiding Third-parties, Brokerage services, Unreliable Transactions, Settlement between owner and tenant, etc. A complete overview and design of the decentralized application with a smart contract is obtainable, and then implementing a use case for leasing/renting residential and business buildings is examined. In this proposed experiment, the solidity smart contract helps to save Brokerage charges and trustiness, reducing intermediaries in distributed and decentralized public ledger and storing all these transactions in a blockchain logs file between owner and tenants.

However, one of the paper's flaws is that because Blockchain transactions are transparent to everyone, users' transaction information could be maliciously abused. The second drawback is that the owner has entire authority over the contract while the tenant has very little, allowing the owner to engage in unfair practices in some cases. Another disadvantage is that all user data is saved on Blockchain, which is expensive storage, costing $17,000 for 1 MB of data. The final issue is that there is no verification system in place to increase public trust, which might lead to malicious exploitation of the technology. All of the above disadvantages are important and have an impact on the blockchain platform's user experience and data security.

2.2 A Secure Data Sharing Platform Using Blockchain and Interplanetary File System, Muqaddas Naz, Fahad A. Al-zahrani.

This research proposes a blockchain-based housing rental system that enables for peer-to-peer listing information exchange without the use of an intermediary. Traditional lease agreements are digitally converted into smart lease contracts, speeding up the leasing process and maintaining transaction records for the leasing process, offering legal protection for tenants and owners. Smart contracts and IPFS (Interplanetary File System) are among the cutting-edge technologies used in the new system. IPFS is used to store the listings data. A smart lease contract is designed to make the property leasing process traceable and transparent using Ethereum's Smart Contracts. The solution in this paper is based on Ethereum's Smart Contract, IPFS and Oraclize services. The blockchain, on its own, is an

expensive data storage medium. It is not suitable for storing digital content of listings information with multiple images. This article demonstrates how Ethereum's smart contract and IPFS can work together to store listing information, and how IPFS hashes can be stored on blockchain smart contracts for traceability and authenticity.

This paper introduces us to the alliance chain, a partly decentralized system used to verify smart contract transactions. It cuts the transaction cost down to just $2 from the previous $17,000. However, there are still some drawbacks, such as the lack of security protocols for securing the user's private information and transaction. Also, this is a weakly centralized system that can be used to verify smart contract transactions, resulting in biased results in certain conditions. This approach is highly susceptible to disputes as the tenant pays the whole transaction amount upfront. Here, it managed to solve some of the drawbacks of previous papers, such as storing data on IPFS, which is way less expensive compared to blockchain.

2.3 PPHR: Blockchain-Based Privacy Protection House Rental System, Mingchong Li, Xiaolei Dong.

This article proposes to provide Blockchain and smart contracts for a specific domain, namely real estate, in order to handle issues such as avoiding third parties, brokerage services, reliable transactions, owner-tenant settlement, and so on. There is a full analysis and design of a decentralised application with smart contracts, as well as an examination of the practical use case for leasing/renting residential and commercial properties. In the decentralised system, it presents a cryptography-based mechanism for validating the tenant and owner. The study uses cryptographic technologies such as zero-knowledge proof (zk-SNARK), digital signature, and others to achieve the goal of privacy protection. It also introduces a trusted authority to control malicious behaviour, hence improving the user experience.

This paper addresses the data security issues that arise by using a cryptographic solution. However, there is no mention of a new approach for resolving owner-tenant issues. Another problem is that no information about the smart contract is provided. As a result, we have no idea how the smart contract works, which leads to a lack of transparency. The last point is the most important: the concept of trusted authority has not been fully described. Although the article mentions a trusted authority, it is unclear who will choose the trusted authority and how the trusted authority would verify users.

CHAPTER 3
PROPOSED SOLUTION

3.1 PROPOSED SOLUTION

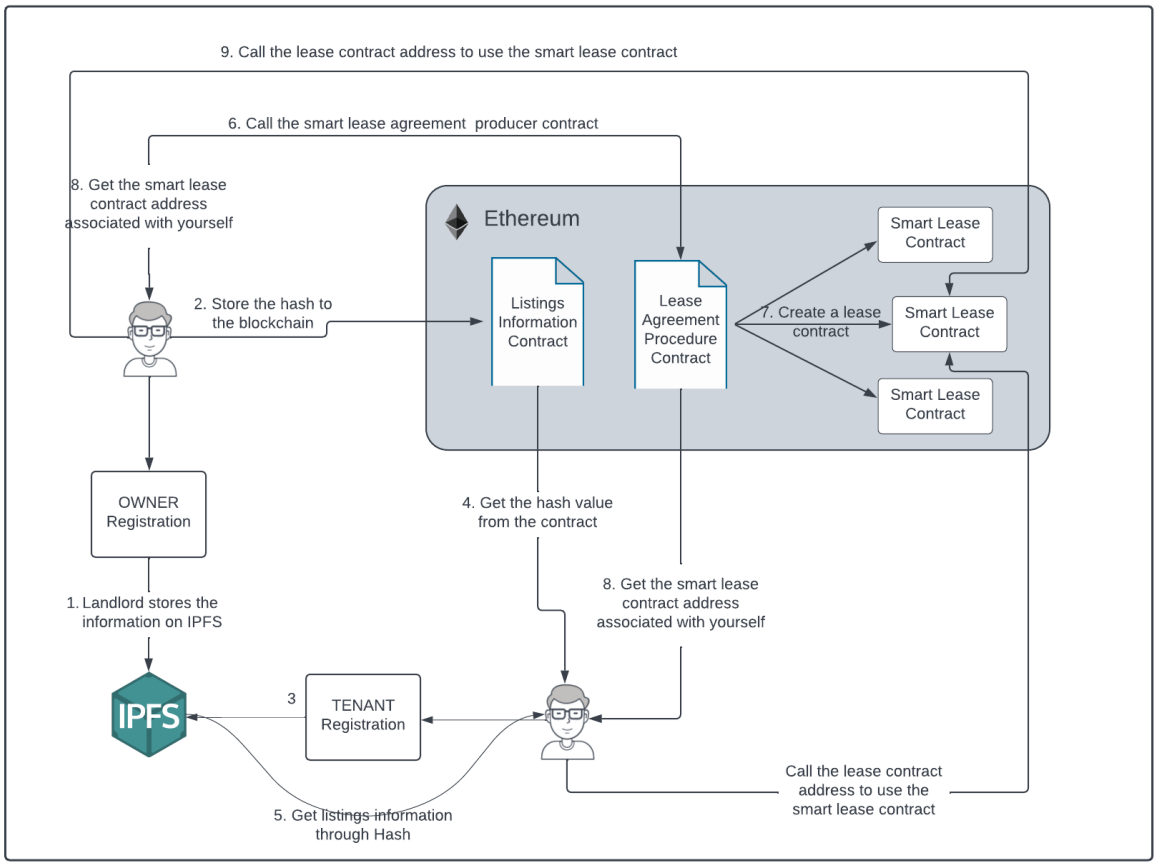


Fig 3.1: Proposed Solution

Figure 3.1 shows the core operating mechanism of the Ethereum Smart Contract, IPFS, and Oraclize services in this system, and the interaction process between smart contracts and participants.

Initially the owner is registered on the blockchain with the help of admin which works as trusted authority in this case. Similarly the tenant is registered on the blockchain using the same mechanism .

As seen in the given figure the owner then sends the listings information stored in the JSON format to IPFS. After the IPFS obtains the request it returns the hash key to be stored in the listings information contract. Along with this the owner also stores the pincode on the blockchain after. The tenant obtains the listings by visiting the listing information contract,

filters them according to the pin code and checks the corresponding listings with help of the IPFS key .

The tenant looks for the best suited place according to his needs and sends the request to the owner once the owner agrees the smart contract execution starts and the smart lease contract is executed and the payment process starts. The whole smart contract ends when the tenant leaves the house and the house again becomes available for the listings .

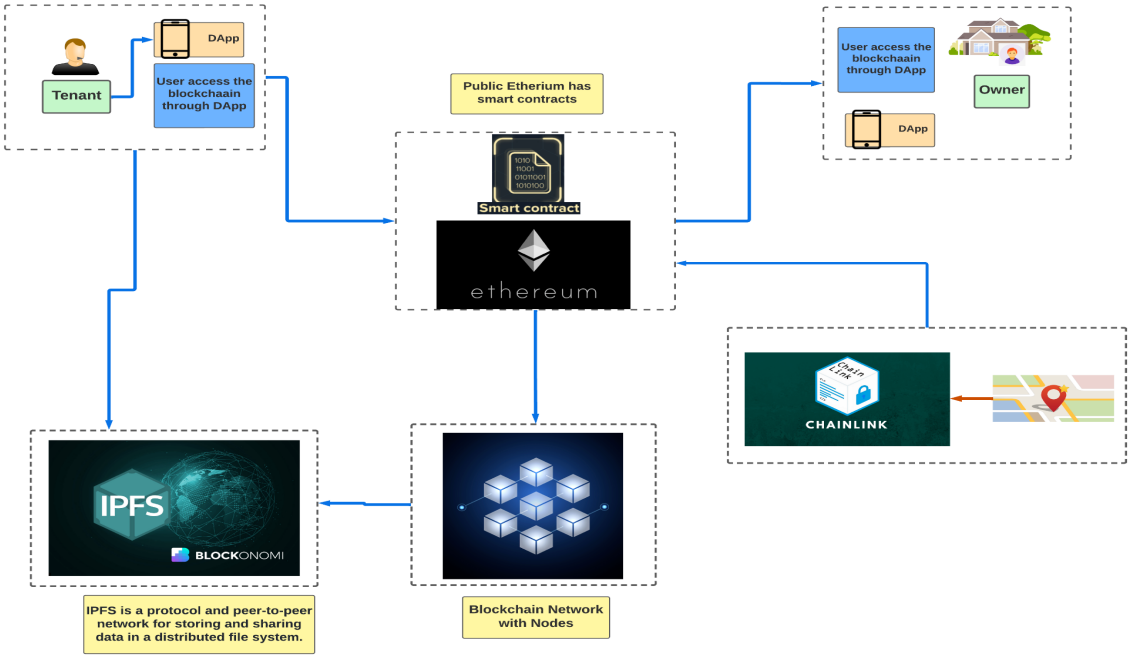


Fig 3.2 : Conceptual Diagram

3.2 REGISTRATION PROCESS

The registration process refers to registering the users i.e. the tenant and the owner on our platform for utilizing the services of our solution.

Owner registration : The owner visiting our platform for the very first instance has to undergo the registration process. Owner visits the platform and he has to provide verification details of himself/herself for security measures. The verification details require the owner's name, PAN details , Crypto wallet address and a government certified document such as aadhar card. This data is encrypted in the portal and is stored on a partially centralized database for the time being. The portal admin encrypts the data through a key and verifies the owner . After successful KYC verification he/she is added to the blockchain and the owner gets the access to property registration.He/she is now required with property registration details like pincode and IPFS hash key. And these details are finally stored on the blockchain.

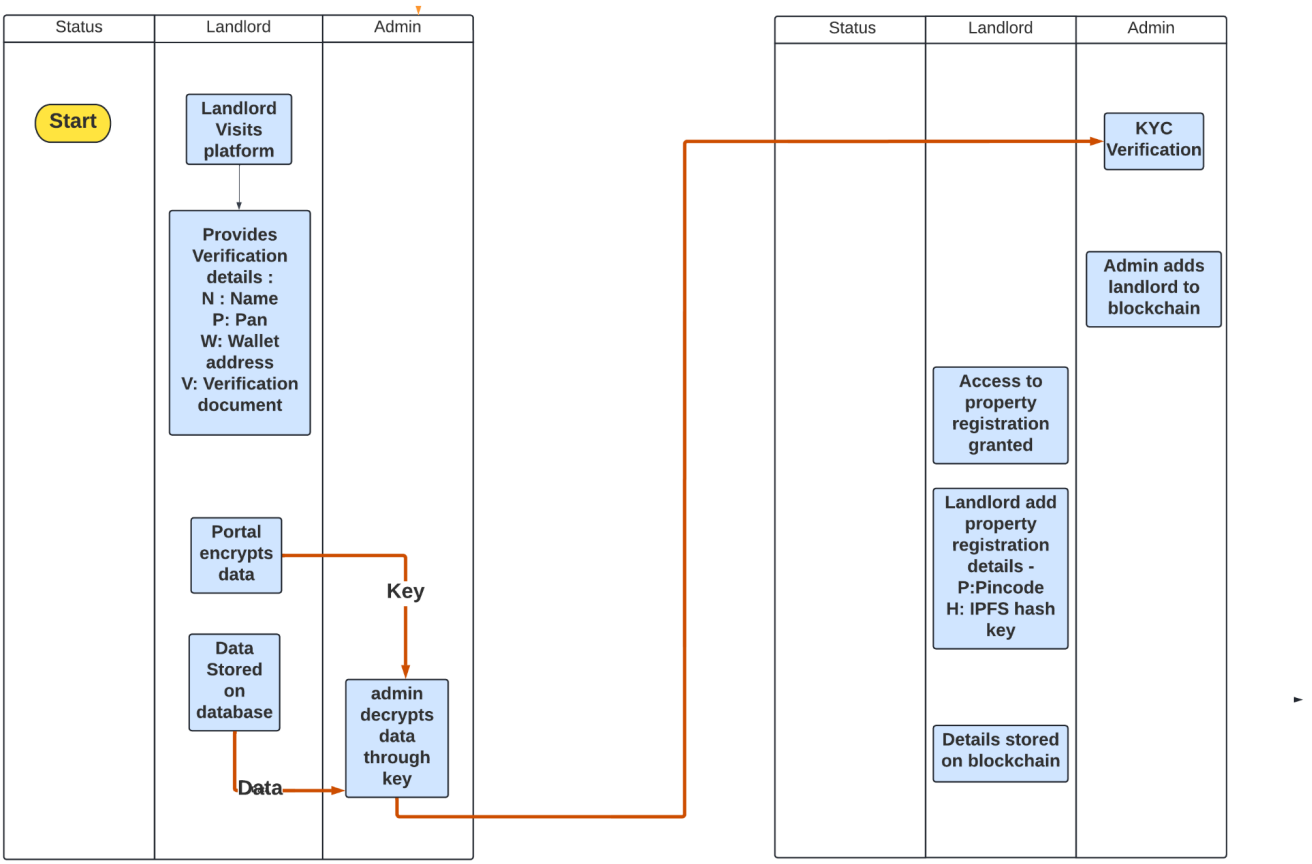


Fig 3.3: Owner registration algorithm

Tenant registration: The tenant visiting our platform for the very first instance has to undergo the registration process. tenant visits the platform he has to provide verification details of himself/herself for security measures. The verification details require the owner's name, PAN details, Crypto wallet address and a government certified document such as Aadhar card. This data is encrypted in the portal and is stored on a partially centralized database for the time being. The portal admin encrypts the data through key and verifies the tenant. After successful KYC verification he/she is added to the blockchain and the tenant gets the access to property listings. He/she is now required to filter property details through IPFS hash key and is required to choose the desired property and send the request.

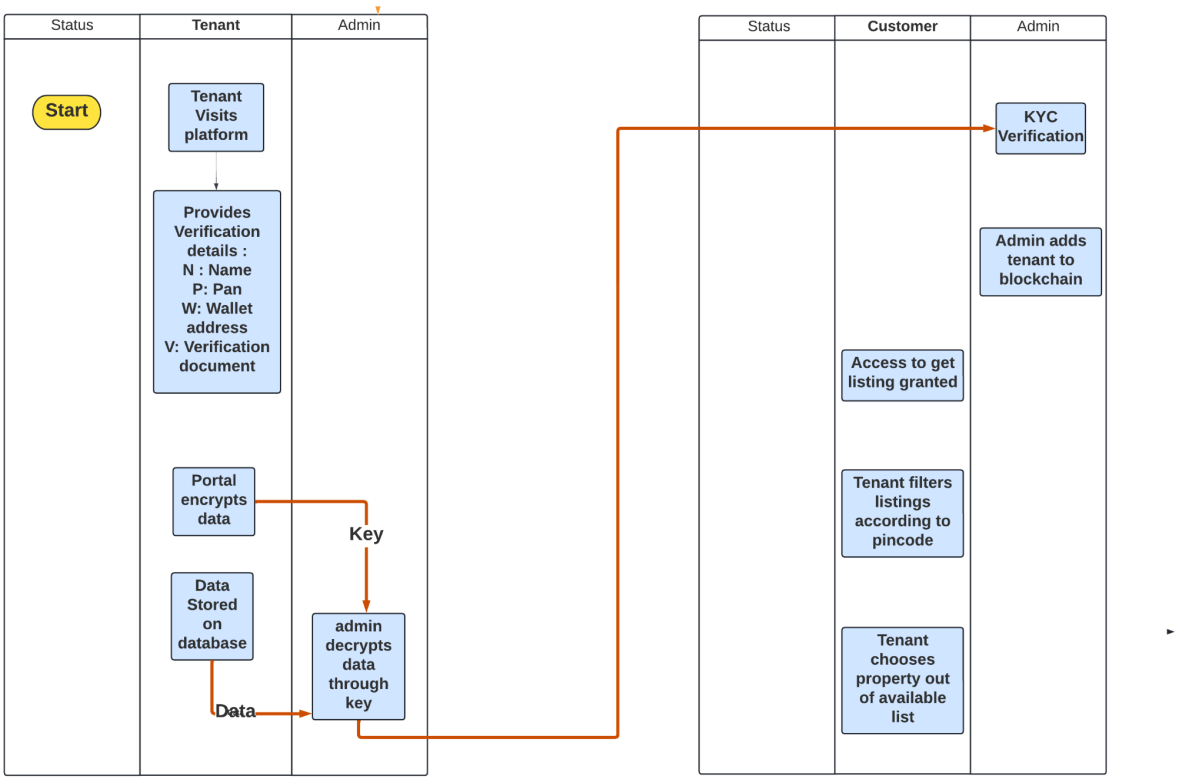


Fig 3.4 : Tenant registration algorithm

3.3 FUNCTIONS IN SMART CONTRACT

We classify the contracts proposed into three groups using the module function division: listings contracts, leasing agreement producer contracts, and smart lease contracts. In this section, we'll go through the details of each of the three contracts:

1. Listings Contract (LC):

It's used to keep track of the hash of IPFS's listing information. The owner has authority over whether or not the hash is accessible to the public. As a result, there are three statuses for the hash:

a. **Unavailable Status:** If the owner does not want to rent the house or it is being renovated, we can set the status of the current listing information hash to unavailable-status via the listing information contract, and the hash will be unavailable to the outside world.

b. **Rented Status:** When the residence is rented, the owner can mark the current listing as rented, preventing the hash from being obtained by the public.

c. **Available Status:** The house is available for rent, and the hash may be found outside.

2. Lease Agreement Producer Contract (LAPC):

To build a smart lease contract, the owner will send information regarding the leasing process, such as the tenant's public key, lease duration, rent, deposit, and lease date. The created contract address will be maintained in the lease agreement producer contract, and the participant will only be able to access the smart lease contract address that is associated with him, making the smart lease contract traceable and manageable.

3. Smart Lease Contract (SLC):

In the leasing procedure, there will be five different statuses: signing the contract, paying the deposit, renting the property, returning the deposit, and completing the contract. The lease procedure status and the refunded deposit status are sub-statuses of the contract in these five statuses. A rental bill is generated throughout the leasing process, and it has three statuses: pending record metre status, paid status, and take out the rent status. The owner is responsible for returning the deposit to the tenant at the end of the lease. The amount of the deposit that is repaid is determined by the owner. The tenant must determine whether or not to accept the owner's offer of a rental deposit. As a result, there are four different states for returned deposits: set the refundable deposit amount, waiting for confirmation, unaccepted status, and accepted status. Because each period of bills must be created automatically in the lease contract, it is necessary to send Ether into the smart lease contract in order to run the smart contract. Activating contract status is the name for this process.

3.4 SMART LEASE CONTRACT STATUS

The operation process for the six smart leasing contract statuses is as follows:

1. Activate contract status: Because the Oraclize service consumes gas during operation, the contract requires a particular amount of ether to be delivered. The owner transfers enough ether to the contract to change its status from inactive to active. The present contract is not activated, and this action can only be performed by the owner.

2. Contract status: The tenant can review the contract's conditions. You can sign the contract and change the status to signed if the tenant agrees to the provisions of the owner's lease agreement. The tenant is the only one who may perform this operation, and the current contract is not active.

3. Pay the deposit status: To bring the contract into action and change the contract status to paid deposit, the tenant must pay the deposit amount specified in the contract. This operation can only be carried out by the tenant, and the deposit for the current contract has not yet been paid.

4. Rental process status: The most time-consuming part of a smart rental contract is the rental process. The lease will automatically generate bills for the first period once the contract comes into effect. The rental bill for each succeeding period will be automatically created by the Oraclize timing service on a monthly basis, based on the leasing date of the contract as the collection date.

a. **Pending record metre status:** This is the leasing bill's initialization status. (Note: because the tenant's first-period rent has not yet generated hydropower, the first-period lease status is unpaid, and the tenant merely needs to pay the rent.)

b. **Paid Status**: Based on the cost of the settled bill, the tenant sends an Ether to the smart rental contract. The tenant's rent is saved in the smart lease contract, and the billing status is changed to paid. The tenant is the only one who may do this activity, and the lease bill status is settled.

c. **Take out the rent status:** At any moment during the smart lease contract, the owner can take out the rent paid by the tenant, and the lease bill status is changed to the status of the rent has been taken out. The owner is the only one who may do this operation, and the leasing bill is paid.

5. Return deposit status: Depending on whether there is any loss of fixed assets during the lease period, the owner will take the appropriate fees from the contract deposit. This charge will be discussed with the tenant, thus there will be four different statuses during the deposit refund.

a. Set the refundable deposit amount: The owner determines the pre-returned deposit and changes the status of the returned deposit to "wait for confirmation." Only the owner can perform this operation, and only if the contract status is not "5.4."

b. Waiting for confirmed status: The tenant can accept the amount specified by the owner and change the current status to unaccepted or accept status; however, the operation can only be performed by the tenant.

c. Unaccepted status: If the tenant does not accept the amount of the owner's returned deposit, return to "5.1" and request that the owner reset the amount of the returned deposit.

d. Accepted status: When tenants choose to accept, the contract status is changed to finished.

6. Contract completion: The owner and tenant have completed the full lease, and the owner can reclaim the remaining balance and the tenant can retrieve the deposit from the lease contract.

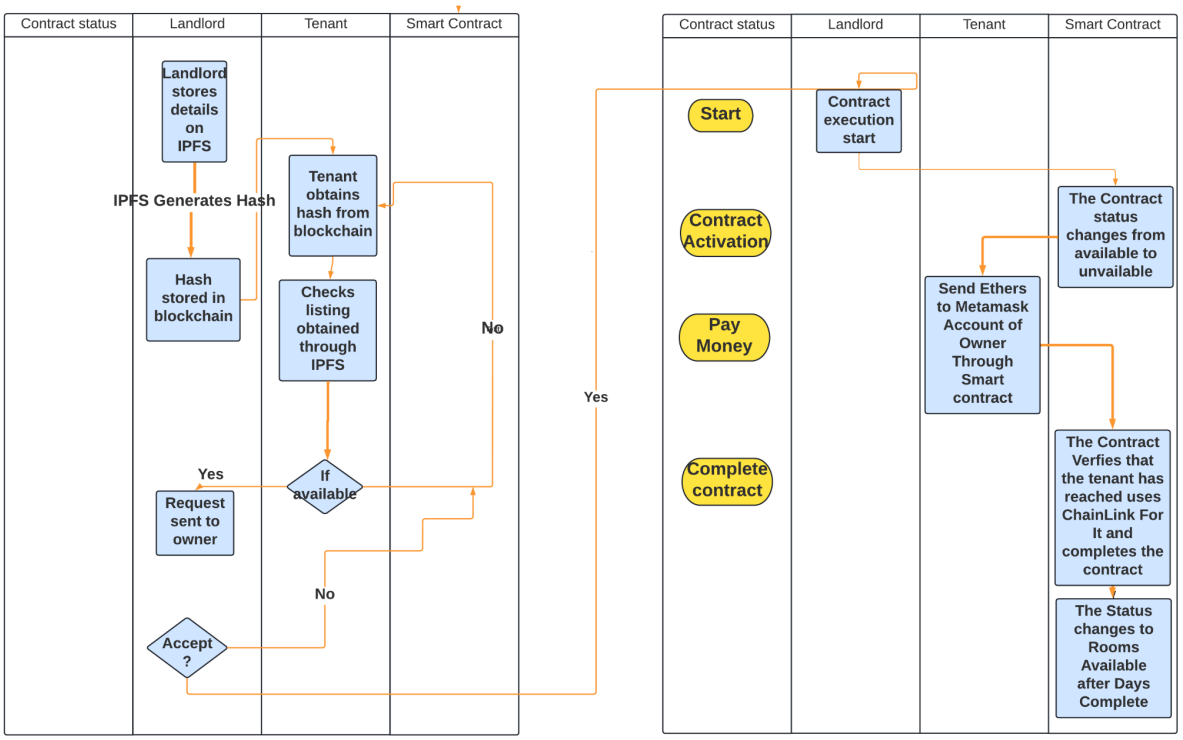


Fig 3.5 : Algorithm Workflow

CHAPTER 4

RESULTS

4.1 RESULTS

The system proposed is blockchain based short-term rental system. In the system the owner registers the property details on IPFS. These details are then stored on blockchain. The interested tenant looks for the listings and the owner approaches the owner. If owner agrees the smart contract gets executed and the money is transferred to metamask account of the owner

The smart contract status changes to paid and the smart contract terminates.

The results for the smart contracts are shown in the figures below:

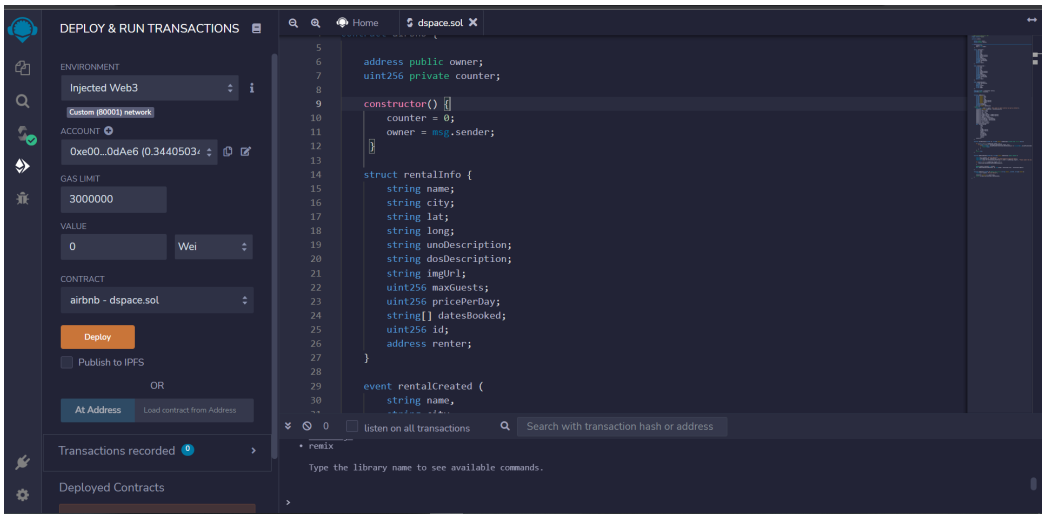


Fig 4.1: Smart contract deployed

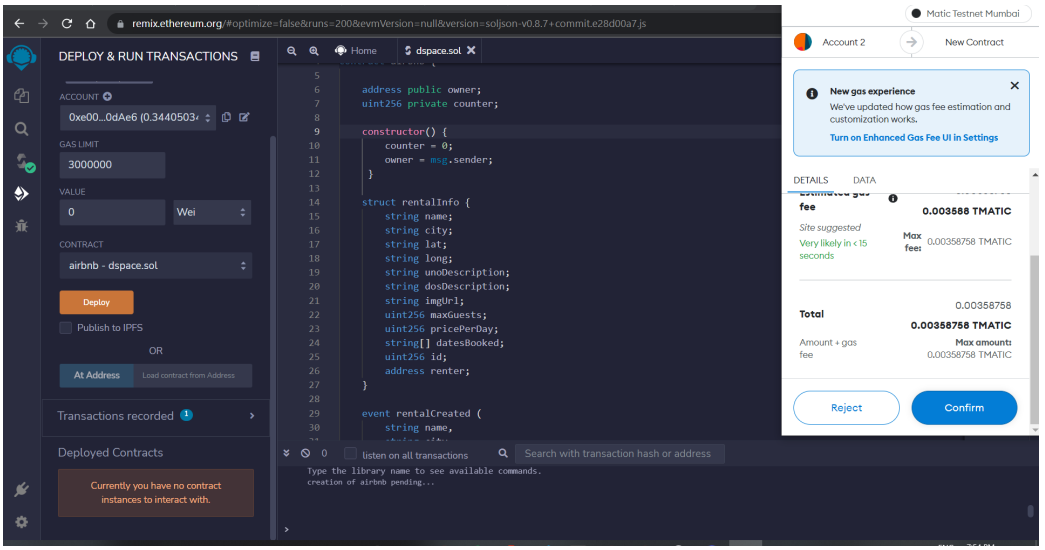


Fig 4.2 : Smart contract deployment transaction made

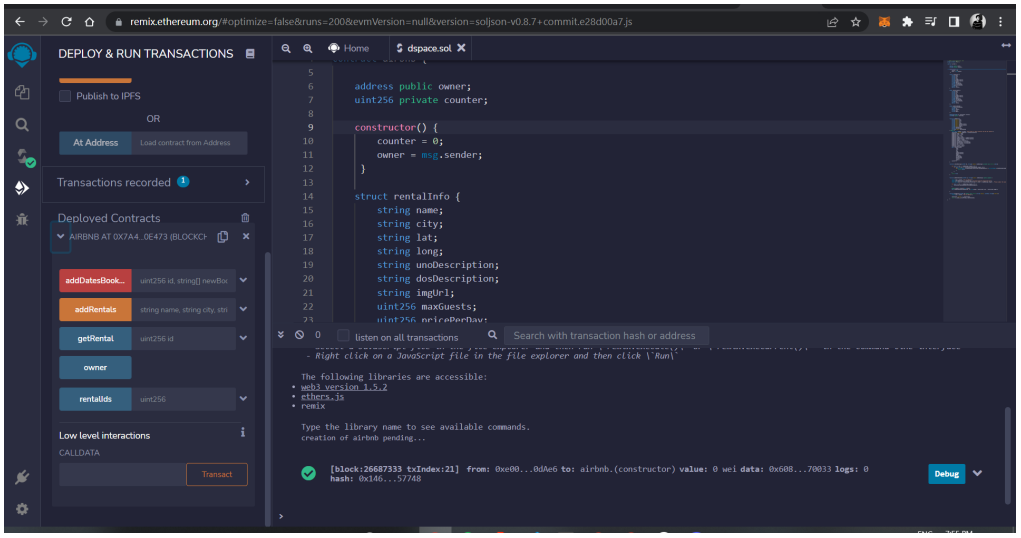


Fig 4.3 : Smart contract successfully deployed

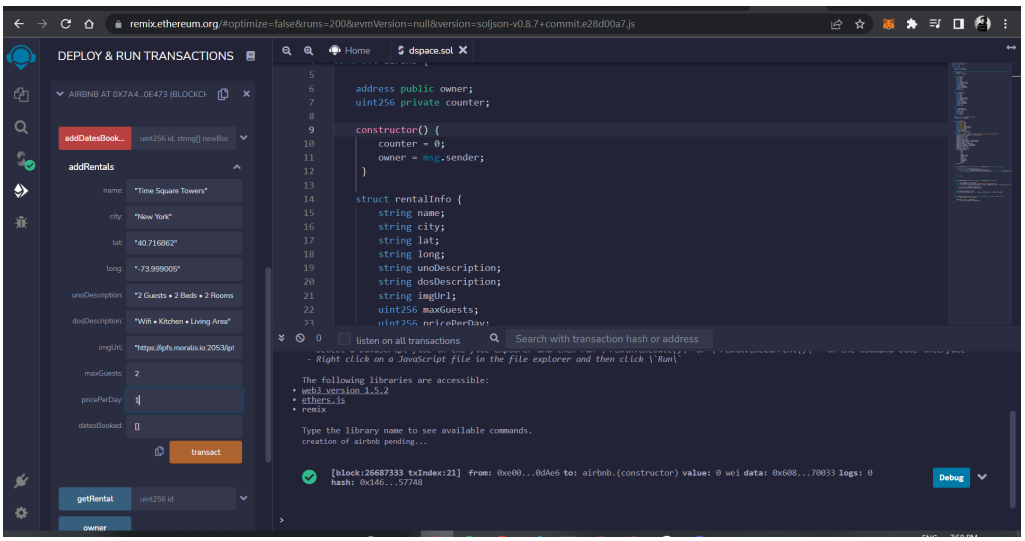


Fig 4.4 : Adding Property listing

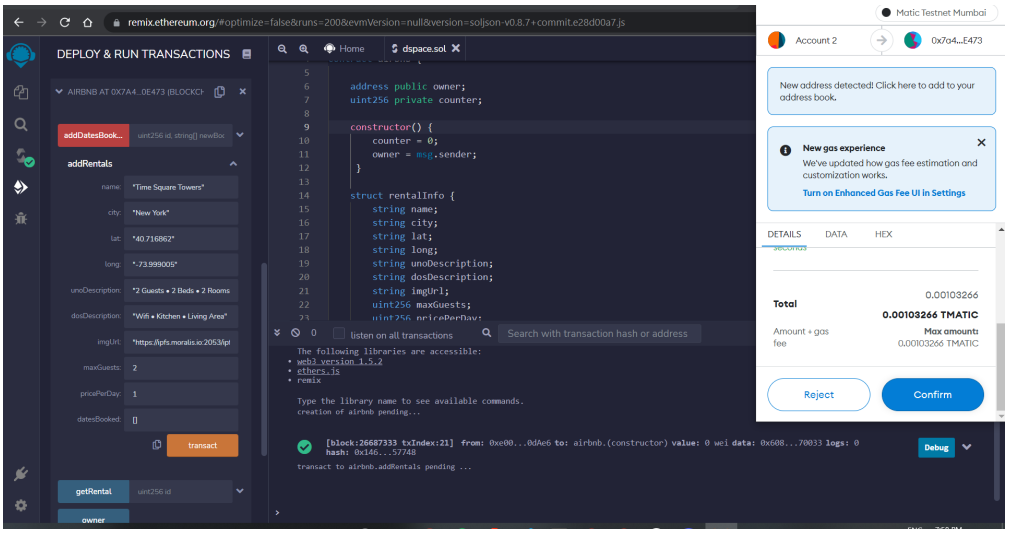


Fig 4.5 : Transaction for Adding Property listing

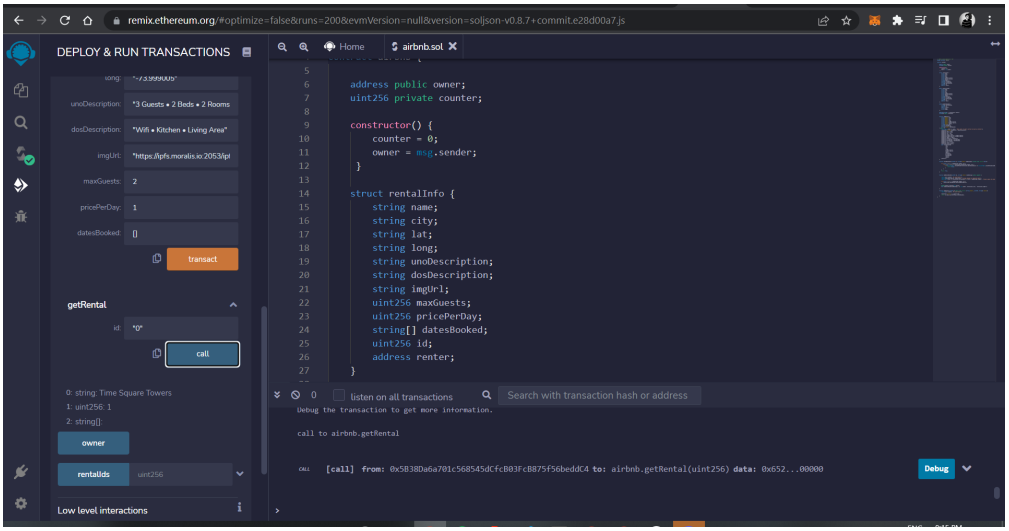


Fig 4.6 : Checking the property listings

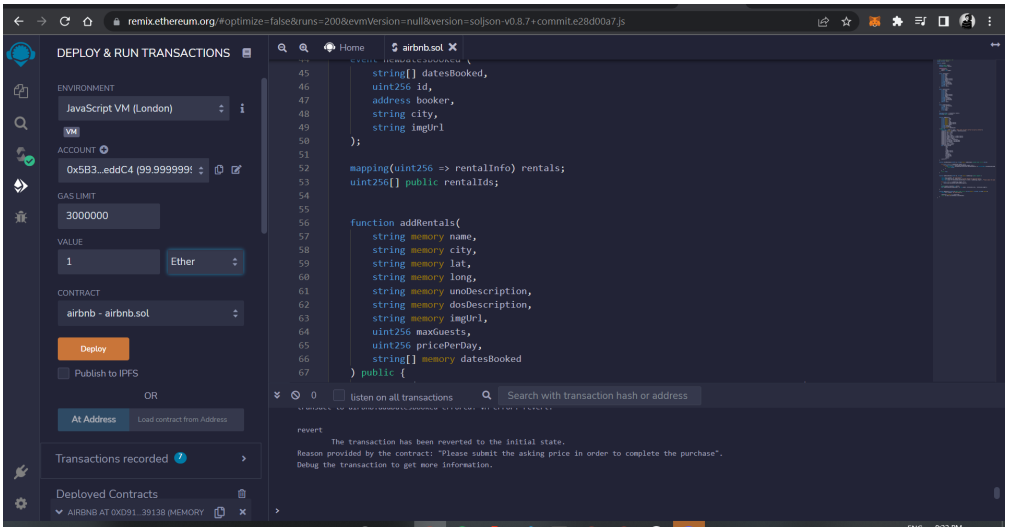


Fig 4.7 : Paying ether for booking

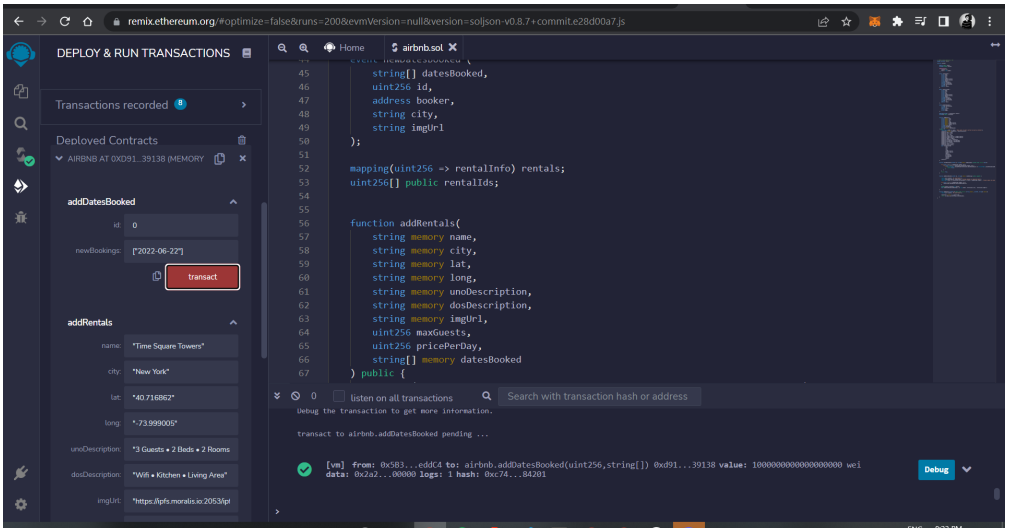


Fig 4.8 : Booking the property with the respective date

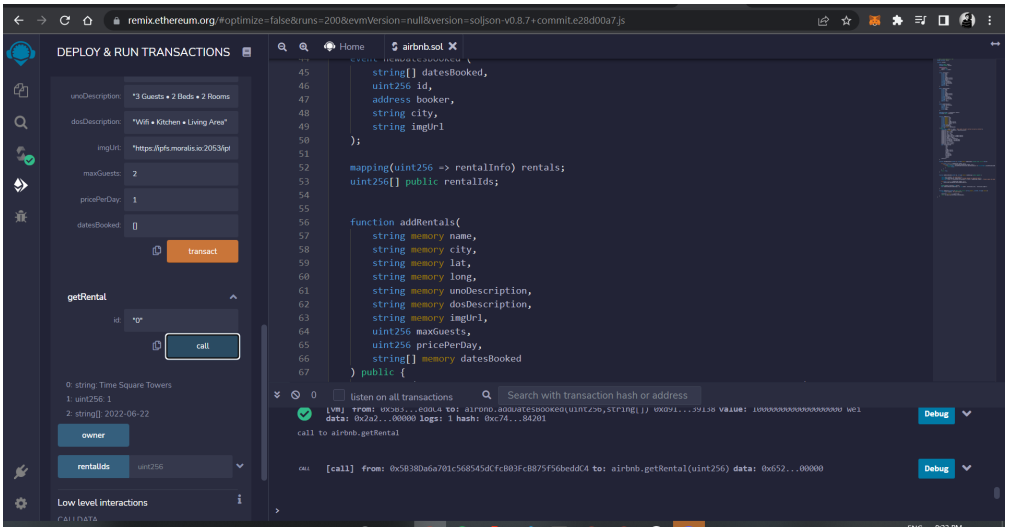


Fig 4.9 : Booking successfully made

CHAPTER 5
CONCLUSIONS

5.1 CONCLUSION

After mainframes, personal computers, the Internet, and mobile/social networks, blockchain technology has seen explosive growth in research and application. It is now considered the fifth disruptive innovation in the computing paradigm, after mainframes, personal computers, the Internet, and mobile/social networks. Following blood credit, precious metal credit, and central currency credit, it is the fourth major milestone in the evolution of human credit (Swan, 2015). Many previously unthinkable things are now achievable thanks to blockchain technology. The blockchain-based housing rental system has provided an excellent example of how blockchain technology may be used. The method leverages the blockchain to exchange listing information, preventing huge corporations from controlling the market price through a large number of users. The concept creates a genuinely decentralised space rental system that eliminates the need for hefty intermediary fees.

The real-time publishing of peer-to-peer listings and listings is made possible by this method. During the rental period, the system changes the traditional leasing method into a manner of coding for both the owner and the tenant using the Ethereum Smart Contract. The contract can only be carried out in the manner in which it was written. The contract protects both the tenant and the owner by permanently preserving all transaction information and records of the tenant and the tenant during the leasing process.

5.2 FUTURE PROSPECTS

In this paper we have successfully proposed solution which will help us to build a truly decentralized space rental system however there is still scope of improvement in the following areas :

1) **Improving Data Security**: Currently the transaction details are getting stored on blockchain which is publicly available in order to add an extra layer of security and privacy the concept of Zk-Snark can be used to conceal the transaction details.

2) **Alliance Chain for User Verification** : Currently a single admin i.e the deployer is responsible for user verification this system can be replaced by the alliance chain. The Alliancechain network is responsible for recording transaction information, authenticating housing source and personal identity information, and putting on chain record of leasing situation.

3) **Improving Smart Contract Protocol** : The Current smart contract covers almost all the cases but this can be further improved with the use of Upgradable Smart Contract as new features and changes get introduced upgradable smart contract helps in updating the protocol and make changes in the smart contract code to make it more robust .

4) **Introducing Rating System** : The current system lacks a rating system to rate the tenant and the owner's experience. In the future, with the help of machine learning, a dynamic rating system can be introduced which will help improve user experience.

REFERENCES

Research Papers

1. Yu, Y., Dong, Y. & Guo, X., 2018. Pricing for sales and per-use rental services with vertical differentiation.
2. European Journal of Operational Research, 270(2): 586–598.
3. Zhuang, W., Chen, J. & Fu, X., 2017. Joint dynamic pricing and capacity control for hotels and rentals with advanced demand information. Oper. Res. Lett.
4. Satoshi Nakamoto. (2018) “Bitcoin: A Peer-to-Peer Electronic Cash System” https://bitcoin.org/bitcoin.pdf
5. Qingshui Xue1*, Zongyang Hou1, Haifeng Ma1, Haozhi Zhu2, Xingzhong Ju2, Yue Sun2
6. Ethereum White Paper, 2015. A next-generation smart contract and decentralized application platform. Available at: https://github.com/ethereum/wiki/wiki/White-Paper.
7. Wood, D., 2014. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Available at: https://gavwood.com/paper.pdf
8. Benet, J., 2014. IPFS - Content Addressed, Versioned, P2P File System. CoRR.

Links

1. Deloitte. (2016) What is Blockchain? https://www2.deloitte.com/content/dam/Deloitte/uk/
2. Ethereum Documentation https://ethereum.org/en/
3. Introduction to Zk-snark https://consensys.net/blog/developers/introduction-to-zk-snarks/