

# **EthStates: Smart Contracts for Decentralized Real Estate Transactions**

**Yin Lam Lai**

y2lai@ucsd.edu

**Viraj Lohia**

vlohia@ucsd.edu

**Eddie Ho**

boho@ucsd.edu

**Ho Kiu Lee**

hkl002@ucsd.edu

**Rajesh Gupta**

rgupta@ucsd.edu

## **Abstract**

This report outlines our investigation and methodology for designing and implementing Real Estate transactions on a blockchain. We start by outlining the potentials of Blockchain and why we chose Real Estate(RE) as the topic we want to build our project on in Section 1: Introduction and Context, followed by an overview of the Technological framework we used in Section 2: Methods, followed by some of the results we achieved in Section 3: Results. We conclude with a brief overview of the progress made while building our project in 4: Conclusion, followed by Limitations and Future Developments in Section 5.

Code: [https://github.com/YLSphere/DSC180\\_ethstates](https://github.com/YLSphere/DSC180_ethstates)

# Table of Contents

1	Introduction and Context . . . . .	4
2	Methods . . . . .	5
3	Results . . . . .	15
4	Conclusion . . . . .	15
5	Limitations and Future Work . . . . .	16
	References . . . . .	17

# **1 Introduction and Context**

## **1.1 Introduction**

Blockchain is often thought to be synonymous with cryptocurrencies and has a very mixed public perception. Nonetheless, Blockchain is a secure and decentralized way to record and verify transactions, providing transparency and immutability to digital data across a distributed network of computers. In the quarter, we first explored the different applications of blockchain carefully analyzing the most optimum use cases of blockchain and smart contracts and current systems which can be improved with blockchain. Once we finalized our project topic, we went in-depth to educate ourselves on the different challenges involved including legal and privacy steps we needed to take.

## **1.2 Context**

In the current day and age, transactions are made not only in-person but also online as well. However, as the internet of all things grows, concerns also grow as well, such as security, speed, and privacy. According to statistics, online payment fraud has led to an estimated 41 billion U.S. dollars lost globally from 2022 and is expected to grow to 48 billion U.S. dollars by the end of 2023 [3]. Despite the growing concerns about internet privacy, many solutions have been innovated to counteract the current situation, namely Blockchain. Blockchain is a decentralized and distributed database that is shared among a group of computer network's nodes, which enables secure and transparent record-keeping of digital transactions [4]. The key feature of Blockchain is that data circulating within the network is stored in blocks that are linked together via cryptography, and the data, once appended in the blockchain, is immutable. This aspect reduces the concern of data being stolen or manipulated, in addition to the need for a centralized party to oversee and reg-

ulate all transactions and data circulating within a system, which also reduces costs and potential human mistakes.

Real estate is one of the biggest assets to be traded in the United States. In 2022 alone, U.S. home sales reached 5 million, and the year before reached 6 million [5]. Given the popularity of buying and selling properties, there needs to be a medium that allows both buyers and sellers to communicate, negotiate, and exchange all necessary documents required to complete a transaction. The real estate agent, or the broker performs these duties; from communicating on behalf of the buyer and seller to managing escrow, all real estate transactions require a licensed real estate agent to facilitate them. However, with the presence of the intermediary, there are also disadvantages in parallel with any modern-day transactions. Namely, one issue is time and money; as all communication is done via a third party and not by peer-to-peer, coordination will be delayed with the need for a third party to relay the messages and the additional cost it requires. Most importantly, all information, including but not limited to a buyer or seller's financial records, property history, and all sensitive personal information is relayed to each other via the agent, thus becoming accessible to the third party who is responsible for transferring this information to both buyer and seller. The information is put at risk, as the intermediary can see it, or in the worst case, a data breach occurs and all personal information is leaked without any insurance.

## 2 Methods

Our project will be developed on the Polygon network, with the Mumbai network as a test network. Our project idea included creating an NFT for each property, minted by the owner and stored in their metamask wallet, symbolizing property ownership and would be the token which is also listed on the marketplace to help in transactions. We also use

smart contracts to complete transactions through our marketplace, be it a sale transaction or a financing transaction. To develop our Ethereum-based ERC 721 smart contracts, we chose to use Solidity as our main language, with hardhat and remix as our compilers. We used the openzeppelin framework of smart contracts to make use of the existing libraries and frameworks. The main advantages of using Hardhat were that it includes a robust testing environment with the capability to run scripts and use additional plugins for contract deployment. Hardhat also makes it easier to integrate Typescript with React, our choice of front-end dev language. Remix is a Web-based IDE that we use in sync with our github to code and test simple smart contracts in solidity. This is a good tool to use in an incremental development process where we test out each module separately before integrating it with our main app. To support the contracts, we will be using Typescript with React to develop most of the connecting communication from the front end to the back end. Storing data on the blockchain is also very expensive so we would be using InterPlanetary File System(IPFS), which is a peer-to-peer decentralized distributed system for storing and sharing data which is called through an API called Pinata from our backend systems. We will be using structs to store the metadata for each property, one each for Location, Property Features, and Owner details. To be able to work on this simultaneously as a group, we have created a GitHub repository, allowing us to push our changes to the project individually.

## **2.1 Setting Smart Contract in Motion**

The online real estate marketplace will be run through a smart contract through our website. Before we dive into the process of executing the smart contract and completing a transaction, we must define some terminology to distinguish all parties involved in the smart contract. Each party using our real estate marketplace will have their identity verified by logging in with their MetaMask wallet, which contains their Polygon currency and their

unique wallet address. All parties must be verified using MetaMask Wallet to ensure the validity and authenticity of the party responsible and to prevent any scams or malicious intents. For our example, we have three MetaMask wallet accounts, each representing a party involved in the sample transaction. The purchasing party will be referred to as the “buyer”, the selling party will be referred to as the “seller”, and the financing party will be referred to as the “banker”. The seller first enters all information regarding the property he or she wants to sell, including address, zip code, city, state, square footage, bedrooms, bathrooms, and desired asking price. All information related to the property will be then stored as variables in the smart contract, and the smart contract is deployed via our website. As the smart contract is deployed, it will appear as a listing in which potential buyers can browse around and pick the property to their liking. In addition, a non-fungible token (NFT) will be minted and granted to the seller’s MetaMask wallet; the NFT represents proof of property ownership, allowing for verification and ease of transaction. The NFT also contains information that the seller inputted regarding the property listed.

## **2.2 Transaction Process**

Now that the seller has received the NFT and the smart contract has been deployed, the buyer can view the seller’s listing, including information about the property that was previously inserted from the seller. The buyer then can either 1) bid with a price of their preference or 2) pay the price asked by the seller. Through the first method, the buyer can offer the seller a price that the seller has the right to accept or deny the offer. If the offer is rejected, then no transactions occur, and if the offer is accepted, then both parties enter a smart contract agreement. For both methods, if both parties agree to terms of the amount of the transaction, then the smart contract checks whether the buyer has enough money in the buyer’s MetaMask wallet; if the buyer does not have enough money to proceed with the transaction, then the transaction will not proceed, and the smart contract will not proceed.

If the buyer has enough funds in the buyer's MetaMask wallet, then the smart contract kicks in, in which a trade of the NFT from the seller will be transferred from the seller's MetaMask wallet to the buyer's MetaMask wallet. The funds from the buyer's MetaMask wallet will go to the seller's MetaMask wallet.

## **2.3 Financing**

Buyers are also able to request a loan, also known as “funding” from verified accounts that wish to loan out their money via deploying a separate smart contract. The loaning party, also known as “banker” for the sake of this example, can loan out their money as a listing. Before the listing, the banker must fill in the necessary information, such as the amount loaned out, interest rate (APY), and payment terms in months. This information will be stored as variables in the financing smart contract, and once the banker fills in all the information required, the smart contract is deployed and buyers can browse the loan listing on the marketplace. When the buyer can find a suitable loan listing for the purchase of a property, an agreement is reached within the financing smart contract, in which the buyer has to pay the monthly principal and interest rate until all amounts are paid off. As collateral, the buyer has to transfer the non-fungible token, representing the property to the banker. For the loan payment, the smart contract will automatically transfer the amount monthly via the buyer's metamask wallet to the banker's metamask wallet. However, if a buyer fails to make a payment, such as not having enough funds in the MetaMask wallet, the ownership of the property is lost and the non-fungible token of the property will be fully owned by the banker.

## **2.4 Architectural Design**



1. Property structure on blockchain

```
struct Property {  
    uint256 propertyId; - to store the id of property  
    uint256 price; - to store the price of the property  
    string uri; - to store the URI of the metadata on IPFS  
}
```

2. Property metadata on IPFS

```
{  
    owner: string;  
    streetAddress: string;  
    city: string;  
    state: string;  
    zipCode: string;  
    squareFootage: number;  
    bedrooms: number;  
    bathrooms: number;  
    parkingSpots: number;  
    additionalFeatures: string;  
    images: string[];  
}
```

Figure 1: (1)Property structure on blockchain and (2)Property metadata on IPFS

### 3. Listing structure on blockchain

```
struct Bid {  
    address buyer; - to store the address of the bidder  
    uint256 bidPrice; - to store the bidding price  
}  
  
struct Listing {  
    // Sale  
    uint256 propertyId;  
    bool buyerApproved; - to keep track of which state of the transaction is in  
    bool sellerApproved; - to keep track of which state of the transaction is in  
    // Financing  
    uint256 financingId; - to store the current financing contract of the property if there is one  
    // Bidding  
    Bid[] bids; - to store all the bids on this property  
    Bid acceptedBid; - to store the accepted bid chosen by the seller  
}
```

Figure 2: Listing structure on blockchain

#### 4. Financing structure on blockchain

```
struct Loan {  
    address lender;  
    uint256 annualInterestRate; // in percentage (e.g 4.56% = 456)  
}  
  
struct Financing {  
    uint256 propertyId;  
    address loaner; - store the address of the loaner  
    uint256 loanId; - store the id of the loaning plan  
    // Financing details  
    FinancingStatus status; various stages including Pending, Active, Rejected, Default,  
    Paidoff  
    uint256 loanAmount; amount of the loan payment (in wei)  
    uint256 durationInMonths; number of months to pay off the loan  
    uint256 paidMonths; number of paid month  
}
```

Figure 3: Financing structure on blockchain

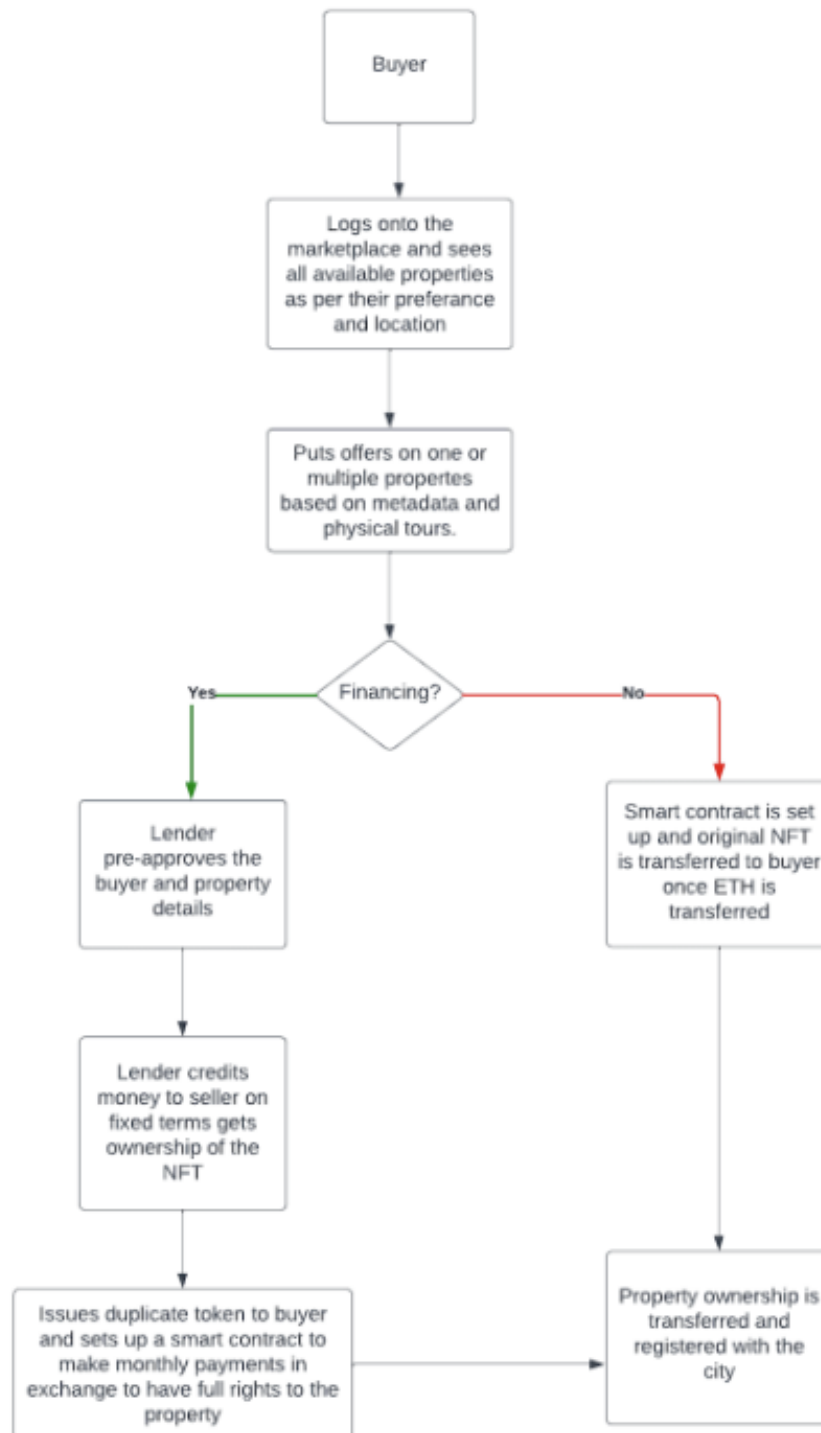


Figure 4: Process Flow for Buyer

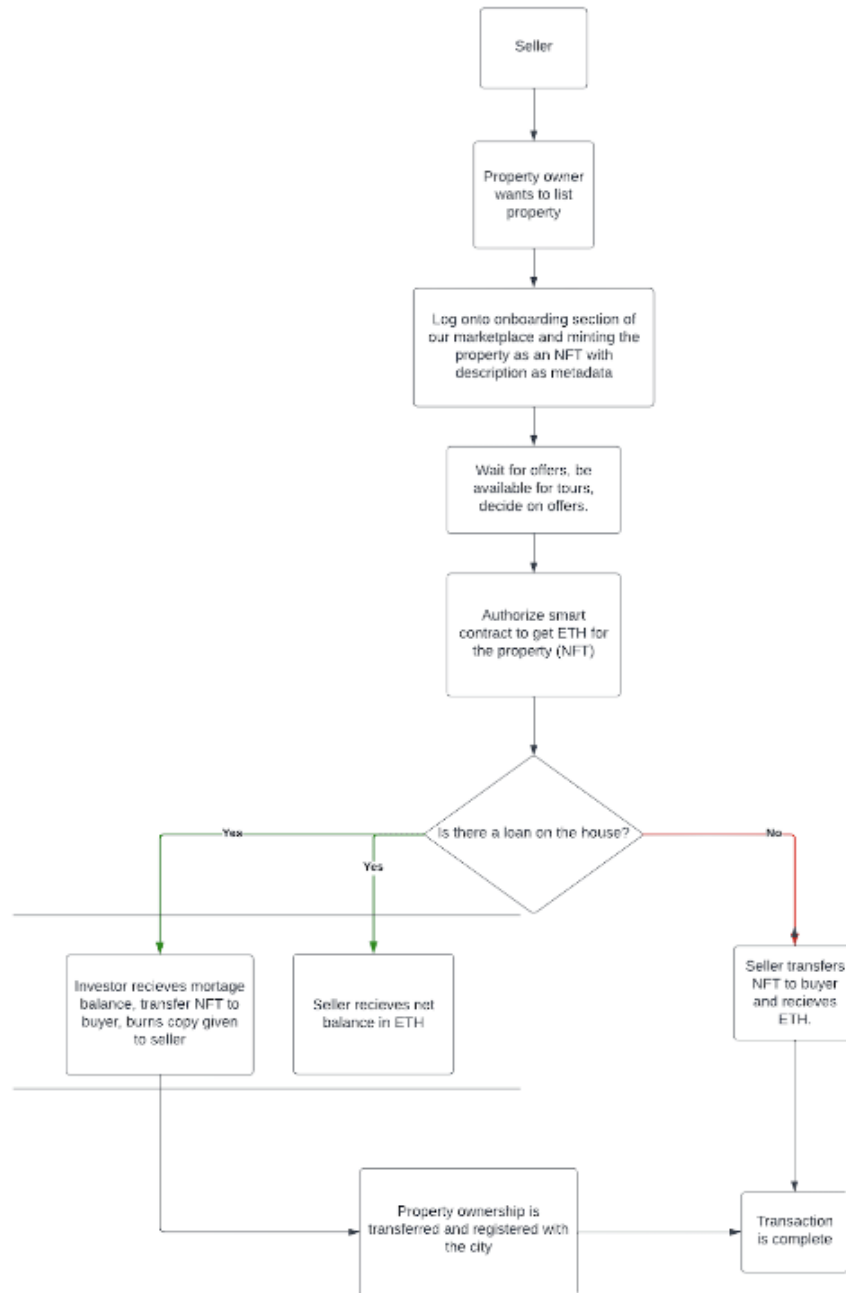


Figure 5: Process Flow for Seller



Figure 6: Process Flow for Banker

### 3 Results

Our marketplace can be found online at <https://dapper-malasada-9683a3.netlify.app/>.

Some features of the marketplace include:

- User login and authentication via MetaMask Wallet
- User can list property by inputting the necessary information required (Address, City, State, Zip Code, Squared Footage, Bedrooms, Bathrooms, etc)
- For every property listed, an NFT is generated and granted to the seller as proof of ownership
- User can bid on properties listed with the amount of their liking
- Seller can accept bids for their listed property based on their choice
- User can also loan out the amount of their liking by creating a listing and filling out the necessary information (similar to seller listing property)

### 4 Conclusion

Our final product, EthStates, is a decentralized peer-to-peer marketplace for real estate property leveraging the technology of blockchain and smart contracts to increase a real estate transaction's security, cost-efficiency, and time efficiency, allowing for a trustless relationship for buyers and sellers. The user-friendly front-end navigation of the website, combined with back-end smart contract mechanisms results in a top-down, simple, and direct process for homeowners and buyers to process real estate transactions safely and securely without the need for a broker to handle lengthy negotiations and demanding fees, overall providing a blueprint of the real estate industry under the governance of decentralization. However, it is believed that blockchain and the concept of decentralization have untapped potential, as the idea that we can exclude the need for a third-party representation in not only real estate but potentially in other industries that currently require mediators such as

banking, insurance, healthcare, education, supply chain, and more. Ultimately, blockchain has laid the foundation for a utopian information system, where concerns about privacy and centralization are eliminated while putting more responsibility and decision-making in oneself.

## **5 Limitations and Future Work**

1. For property authentication and verification, our platform currently uses a Firebase database for cross-verification on the validity of a listed property by a homeowner. To provide a more realistic experience, we input sample property data into our database. While integrating public records API for verification will provide the latest information for property data, there are a lot of gray areas regarding real estate law and regulations that we need further clarification from a regulatory perspective.
2. Currently, the payment methods available on the platform are Ethereum and Polygon. This is because the smart contracts are being hosted on the Sepolia Testnet. In the future, we would like to add more payment methods such as other cryptocurrencies and cash.
3. We would like to implement a live chat function for buyers, sellers, and financiers, which would allow them to communicate and negotiate in real time with each other to eliminate the need for intermediaries to exchange messages.
4. We would also like to enhance our search criteria for buyers, specifically integrating a geolocation search for buyers to look for property listings based on a specific area the buyer desires.



## References

- [1] James Howell *Hardhat Vs Truffle – Key Differences*. <https://101blockchains.com/hardhat-vs-truffle/>
- [2] Sasha Shilina, *What is the InterPlanetary File System (IPFS), and how does it work?* . <https://cointelegraph.com/learn/what-is-the-interplanetary-file-system-ipfs-how-does-it-work>
- [3] Daniela Coppola, *value of e-commerce losses to online payment fraud worldwide from 2020 to 2023*. <https://www.statista.com/statistics/1273177/ecommerce-payment-fraud-losses-globally/#:~:text=E%2Dcommerce%20payment%20fraud%20losses%20worldwide%202020%2D2023&text=According%20to%20estimates%2C%20e%2Dcommerce,billion%20U.S.%20dollars%20by%202023>
- [4] Adam Hayes, *Blockchain Facts: What Is It, How It Works, and How It Can Be Used*. <https://www.investopedia.com/terms/b/blockchain.asp>
- [5] Statista Research Department, *Number of existing homes sold in the United States from 2005 to 2023*. <https://www.statista.com/statistics/226144/us-existing-home-sales/#:~:text=The%20number%20of%20U.S.%20home,from%206.12%20million%20in%202021.>