



Capstone Project Phase A

Real Estate – Crypto

Project 21-2-D-1

Alex Keselman

Michel Abou Hamad skoko216@gmail.com

Maor Grinberg nimnimaor@gmail.com

Contents

ABSTRACT	3
Introduction	3
Background and Related Work	4
Expected Achievements	6
Research / Engineering Process	7
Evaluation/Verification Plan	11

ABSTRACT

Real estate is one of the biggest investments businesses and an investment that is considered safe and profitable. Nevertheless when we talk about real estate deals in today's world there are two main disadvantages making them, firstly it's the brokerage fees that the buyer need to pay for the bank/mediator/lawyers when he wants to buy a real estate and the second one is the long time it takes to make such a deal, it may take weeks to months. In this project book we will discuss why in today's government systems these two disadvantages exist and how we can, by using the Blockchain technology, solve and make the real estate deals more reliable, cheaper and faster. We will explore and explain what the Blockchain is, why it's more reliable and secure even more than banks and government's offices, how it can make real estate deals cheaper by reducing the brokerage fees and faster by making all the transactions and protocols of changing the ownership of an asset using the Smart Contracts in the Blockchain. We will discuss what the meaning of tokenizing assets is and what NFT's are. We will discuss the obstacles that we will face doing it from making the transaction legal by paying the taxes and transferring the ownership of the assets to regulation problems.

We will introduce our final product of the project which is a functional website where users can make NFT's for their assets, how they can advertise their assets on our website and how other users can search assets and request to buy them using cryptocurrencies.

Introduction

In today's economy, in order to carry out real estate transactions, there are many intermediaries in the process who deal in the same transaction. In order for a real estate transaction between two parties to take place, a third party is always involved, such as a bank, mediators, lawyers and various government entities involved in the transaction. Due to this fact the deal is much more expensive because of brokerage fees for each party involved.

The involvement of the various factors creates many delays and bureaucratic processes which cause an extension of the time for executing the transaction, usually lasting weeks to months.

Our goal in the project is to facilitate the execution of real estate transactions and significantly reduce the number of people involved in the transaction so that only both parties (the buyer and the seller) are involved in the execution of the transaction.

Reducing the number of parties involved in the transaction and ensuring that the transaction takes place legally and safely without the need for many intermediaries will result in a reduction in taxes and fees and shorten the waiting times for approving a transaction, transferring funds and ownership of the property.

Our project is mainly aimed at people who want to buy or sell real estate properties quickly and minimize commission payments.

Using the Ethereum platform combined with a Smart Contract, we will streamline the real estate world and shorten transaction processes by creating Smart Contracts for transactions between the buyer and seller and transferring ownership between them, all subject to local state laws.

Using these contracts will not only ensure the transaction and its protection against counterfeiting by using Ethereum Blockchain technology but will also lead to a significant reduction in brokerage fees and execution of the transaction from weeks to a few minutes.

The motivation for the project comes also from the fact that until today there are few websites that let you register your asset as an NFT and to be able to do real estate trading using cryptocurrency. EtherLand is one example of such a website, the company tokenizes famous monuments around

the world. As we mentioned before, real estate businesses are one of the largest markets in the world so we think we will easily find some investors to invest in our product.

In this project book we will discuss the background of the technologies we are using in our project, we will show why they are reliable and secure. Then we will represent how we combine those technologies together into developing our product. We will showcase our final product which is a website and what features it will contain. Then we will discuss how we are going to test and evaluate our product.

Background and Related Work

A Blockchain as it is called is a chain of blocks which contains information. Each block consists of: a record of information, its personal hash and the hash of the previous block. The information stored in the block can vary depending on the properties of the Blockchain such as:

A Bitcoin Blockchain in which each information record in the block contains transactions with information of who is transferring, where it is transferring and what the amount is. When each block is created it has a unique hash that changes each time the block records are being changed, so it will be easily identified.

The third characteristic that exists in each block keeps the hash of the previous block, which makes the network very safe and difficult to fabricate.

The first block in the network is called "genesis block", when someone tries to change something in one of the blocks in the network it changes its hash which makes the other blocks invalid (out of date). However computers today are fast enough to calculate thousands of hashes per second and be able to recalculate the remaining hashes of the other blocks to make the chain valid and up to date again.

In order to prevent this in the Blockchain there is a concept called "proof-of-work", this is a mechanism that slows down the pace of creating new blocks. For example: in Bitcoin today it takes about 10 minutes to calculate "proof-of-work" in order to add a new block to the chain. This mechanism makes it difficult to fabricate blocks because in order to successfully fabricate the block and all other blocks that follows, the fabricator needs to calculate all the "proof-of-work" of the blocks after the fabricated block includes the block itself, it is necessary to do so in order to maintain a chain standardization.

Another security mechanism of the chain is called "peer-to-peer" or in short "p2p network" the meaning is that instead of keeping the chain in one central place that will manage and store information, users in a P2P network that allows anyone who wants to join to get a full copy of the Blockchain, which helps to verify whether a particular block in a particular user network is valid by checking that the block have the same hash like the copies that all other network members have.

This means that if someone fakes a particular block in order to be able to do so they must be able to change that specific block and calculate the "proof-of-work" at least for more than 50% of the network users, which is not possible to do.

The Ethereum Blockchain is a decentralized, open-source Blockchain with Smart Contract functionality. Ether (ETH) is the native cryptocurrency of the platform. It is the second-largest cryptocurrency by market capitalization, after Bitcoin. Ethereum is the most actively used Blockchain up to date.

A smart contract is a computer protocol designed to enable, verify and / or enforce digitally the negotiation or execution of a contract. It is actually a set of commands and conditions, written in

software language and based on Blockchain technology. Smart contracts allow us to transfer Funds, shares and any type of asset or value in a transparent and distributed manner, without a third party or intermediary while executing reliable, traceable and irreversible transactions.

A smart contract works automatically according to the terms and restrictions defined in its specific protocol - when the terms of the transaction are met (such as a specific date or a predetermined share price), the contract is executed immediately and automatically. A "if and then" mechanism that does not require external involvement. Both sides of the contract remain anonymous, but the contract itself sits on the public network log (Blockchain) and is completely transparent - anyone can check the contract and get all the existing information about it. The smart contracts are written in code language (Solidity) and therefore technical knowledge is required to read the actual contract, however the information is accessible to all.

Thanks to these characteristics, Smart Contracts make it possible to reduce the various transaction costs involved in the contract between the parties (such as bank fees), as well as to provide much higher security than the law offers for traditional contracts.

One of the main problems was if they were producing new tokens, users would have to send Ether to the smart contract in order to get several tokens accordingly. In case they were sending a token other than Ether and the smart contract does not know how to deal with the tokens, the tokens sent would be lost and there was no way to return them. So a standard was created to deal with this problem. The standard was created due to the multiplicity of smart contracts that each contract has its own code and functions and in order for the smart wallets to perform the transactions recorded in the contracts they had to create a specific code for each smart contract, hence the need for a common language to all smart contracts.

ERC-Ethereum Request for Comments

ERC-20 is a standard for creating cryptocurrencies - in order to create our own currency, 6 basic functions and 3 non-mandatory functions (name, symbol, and decimals) must be implemented.

The basic functions are:

- **totalSupply** - how many total currencies will exist
- **balanceOf** - Returns the amount of tokens of the given address
- **transfer** - transfers from the total quantity to a specific user
- **transferFrom** - transfer between 2 users
- **approve** - makes sure that the contract can transfer a certain amount to the user in relation to the total amount
- **allowance** - makes sure that the transferring user has enough tokens to transfer the amount to the receiving user

Similar to object-oriented programming, the ERC-20 standard can be compared to an interface and in order to use the standard it is necessary to implement its functions.

This standard solved the issue created by having multiplicity of smart contracts. This standard was groundbreaking and first of its kind but it also had some issues, it was only a guideline and people were free to implement it as they wished.

ERC-20 is intended for use in the creation / production of fungible tokens, the value of each token in the same family is exactly the same.

On the other hand, there is another standard with more functions for implementation that's called ERC-721 standard, which is intended for creation / production in assets / products that are not equivalent to each other, i.e. which are non-fungible (NFT). For example: stocks and rare collections that each item stands at a different value on its own.

Tokens created under this standard are unique and each token created knows who owns it. In addition to the existing functions in ERC-20 standard, there are two more functions that must be implemented in this standard:

- **ownerOf** - the owner of the currency
- **takeOwnership** - transfers ownership of the currency

For example CryptoKitties is a Blockchain game on Ethereum developed by Canadian studio Dapper Labs that allows players to purchase, collect, breed and sell virtual cats. CryptoKitties operates on Ethereum's underlying Blockchain network, as a non-fungible token (NFT), unique to each CryptoKitty. Each CryptoKitty is unique and owned by the user, validated through the Blockchain, and its value can appreciate or depreciate based on the market. CryptoKitties cannot be replicated and cannot be transferred without the user's permission even by the game developers. Users can interact with their CryptoKitties, having the ability to buy, sell, and sire (breed) them. The CryptoKitties concept can be translated for real estate assets where it cannot be replicated and cannot be transferred without the user's permission. This technology can help us create tradeable NFT's where every token represents a unique real estate asset and every token has an owner.

Expected Achievements

In our project we expect to build a functional website where the users can add their real estate asset to the Ethereum Blockchain as a NFT token using a Smart Contract with ERC-721 protocol. The users only need to register their assets with the relevant data, for example land block and plot numbers or the book and page number in the registry and for apartments in shared buildings you must also have the secondary-plot number. Usually the secondary-plot number and apartment number are not the same, then the website using the Smart Contract will create an NFT token for that specific asset, add it to the Ethereum Blockchain and add the NFT to our site where other users/potential buyers can see. Each user can add pictures and relevant information about the asset to the site to make it attractive. Users of the website can request to buy an asset from its owner. Every asset will have its price in Ether and the price can be changed only by the owner and only if the asset doesn't have active buy requests. When a transaction happens our Smart Contract will be able to transfer the expected Ether from the Buyer to the seller plus a small fee that we take. The fee includes Ether that we need to exchange into regular money for paying taxes to the government and a brokerage fee. The amount of the fee is based on the local country laws. The exchange of the Ether to regular money is done using Oracle API for transferring the right amount of Ether to the local currency.

We expect that the transactions will be executed safely as a regular real estate transaction but much faster and saving wasted time on lawyers and bank bureaucracy. The project will include an attractive search engine for apartments that can be bought with the help of our cryptocurrency. It will be possible to filter by: number of rooms, city, house size and price. The project success criterion is to be able to add a real estate asset to our website, the website needs to create an NFT for the specific asset using our Smart Contract and to be able to do transaction between buyers and sellers. The biggest challenge in our project is to be able to make the transactions and trading reliable and to be able to legalize the transactions according to the local country laws.

Research / Engineering Process

Process:

The main research we did was the subjects we mentioned in the previous chapter. We researched thoroughly every subject and technology that is involved in our project and wanted to understand how and what features we need to choose or develop so we can make the main purpose of the project, which is making reliable real estate transactions, really reliable and legal. Firstly we researched what Blockchain technology is, why it is reliable and how we can use it in our project. Then we studied the different types and protocols for developing a token in the Blockchain. After that we studied and researched the Smart Contract technology and its benefits and how it can be implemented in our project. We searched the internet for examples of NFT's and how smart contracts are implemented and we found Cryptokitties which we described in the previous chapter. Finally we talked to our friend's father who works as a real estate agent for years and we asked him how real estate transactions take place in today's world, why a transaction is considered legal and how ownership of the assets are transferred in real life. This research helped us understand the logic and the laws behind real estate transactions and we tried to implement this logic and laws into our project using the technologies we previously described.

The main target in our Project was to find a secured and reliable platform and technology where we could tokenize the assets so the Blockchain was the best fitting platform for us. The Blockchain features that we described in previous chapters convinced us that this technology is the most fitting one for our project and the fact that Blockchains like Bitcoin's are working and proving that this technology is very secure and popular makes it easy on us to choose it. We choose the Ethereum Blockchain because it's one of the most popular Blockchains today that can easily support Smart Contracts and people have already built NFT's Smart Contracts and had a huge success doing it. In our research we wanted to find the best fitting Smart Contract protocol to suit our project so we did research on every Smart Contract protocol to try and find the best one for us. ERC-721 is the best fitting one for us because it describes the assets in the Smart Contract exactly like we wanted to. ERC-721 is already proven to be working and able to produce high quality NFT's and Smart Contracts as we described above, for example the CryptoKitty Blockchain game. We choose a website to be our mediator between our Smart Contract and users because today's internet browsers support a lot of built in cryptocurrency wallets and features that can help us build the website and the users to easily interact with it using known and existing wallets for example the METAMASK browser wallet and etc. Websites are also Accessible to all users from any device and this prevents us from building multiple apps for different devices. We will develop two main Smart Contracts: NFT minting and maintaining Smart Contract and exchange Smart Contract where two users can make the deal between them using it. One of the main constraints in our project is to be able to make the project legal to the government laws. In the end if we really want to be able to deploy our project for real users we need to make the transactions legal by paying taxes and implementing the Smart Contracts to be able to do it the right way. For example if a transaction takes place we need to know if we need to convert some Ether into the local currency and pay the taxes with it or the government is willing to do regulations and add an address that the Smart Contract can directly send Ether to without the need of converting Ether to real money. Also we are depending on government laws to legalize and recognition the asset NFT's. To be able to pay the right amount of taxes and to be able to convert the right amount of Ether to real world money we will use the Oracle Smart contract which can provide in real time the value of Ether in local currencies. For example if we deploy our project in the USA we can by using the Oracle Smart Contract calculate the amount of Ether we need to take from the deal and convert it into USA dollars to be able to pay the taxes. This feature is needed as long as the governments don't make their own official accounts on the Blockchain where we can

easily transfer the Ether to their account without the need of converting the Ether for real regular money currencies.

Product:

Our final product is a fully functional website where users can tokenize their assets using our Smart Contract and being able to add descriptions and photos of the asset into the NFT in the Blockchain. The website will also direct buyers who want to buy assets by implementing a search engine in the website. Users will be able to categorize the assets in the website by: location, price, size of the asset, etc. Users will also be able to send requests for assets that they want to buy and the sellers can easily sell their asset by only accepting the request and our Smart Contract will do everything for them including transferring the money, paying taxes and changing the ownership on the asset NFT.

Asset NFT registration activity diagram:

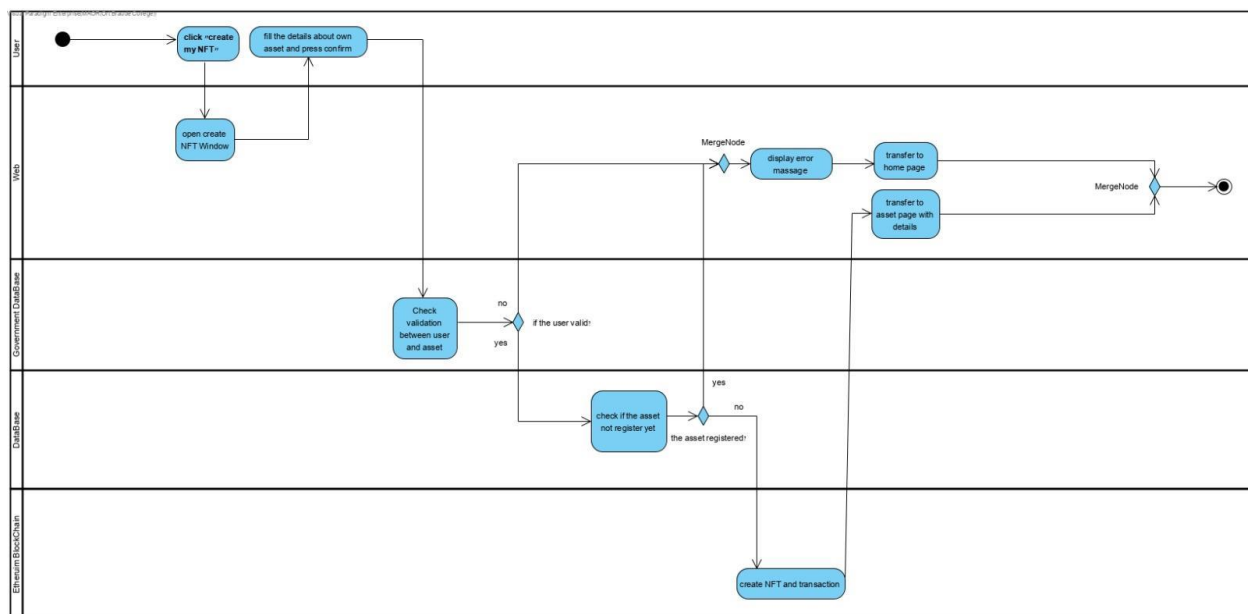


Figure 1

In figure 1 we can see how easy and simple it is for the users to create an NFT and tokenize their asset.

In figure 2 we show the simplicity for the buyers to request and buy an asset in our website using this activity diagram:

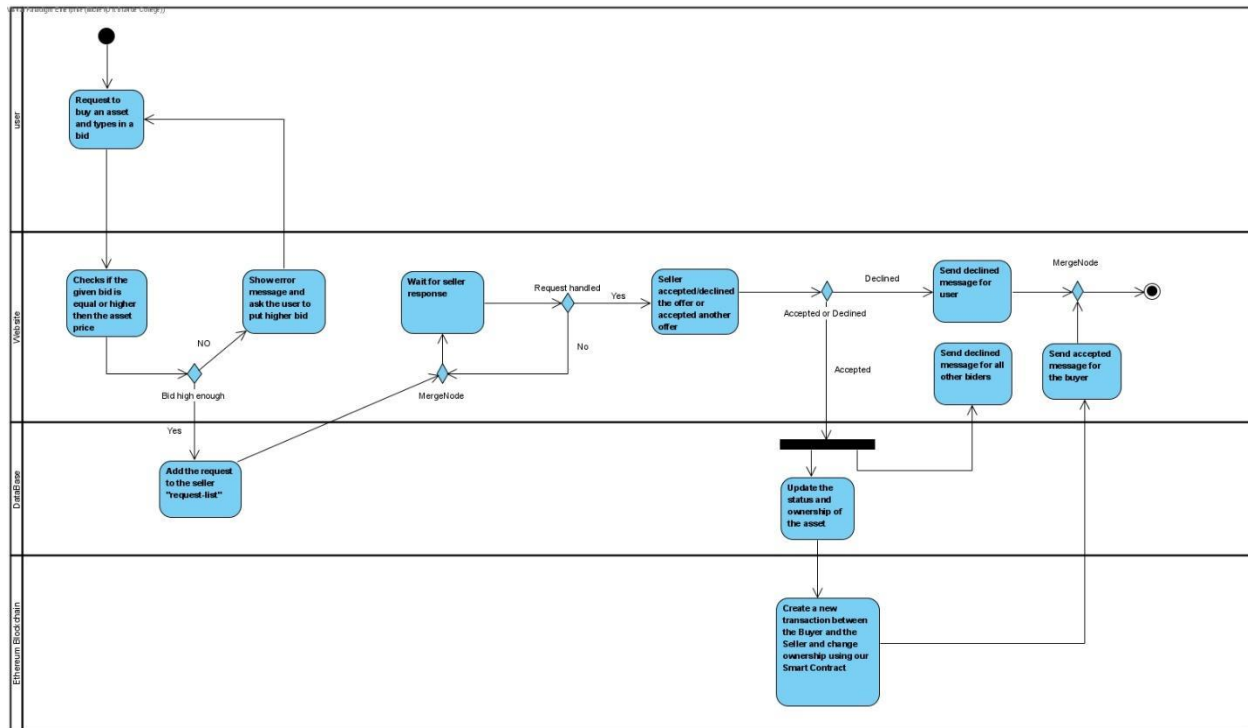


Figure 2

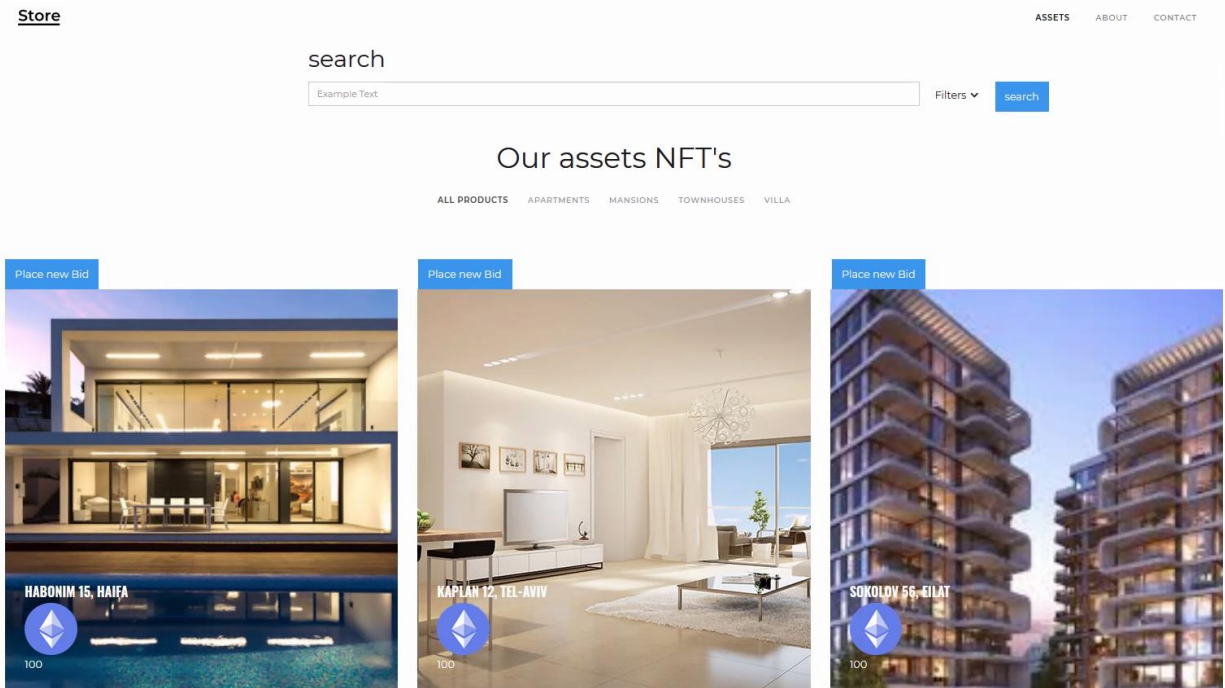


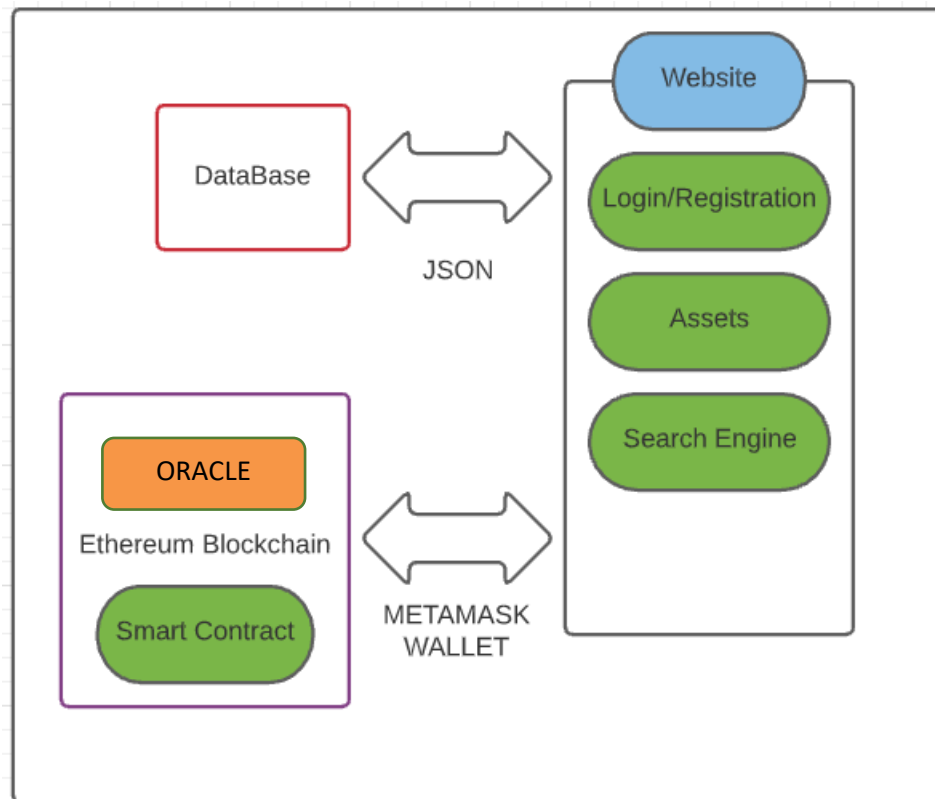
Figure 3

In figure 3 we can see a sketch of our website, you can see the search bar and the option to add a filter beside it. You can also choose what specific asset you are looking for using the quick filter

menu in “Our assets NFT’s” and you can see an example of how we are going to showcase the assets in the website and the button of “Place new bid” where a user can request to buy the asset from the seller. At the bottom left of each asset photo you can see its price and address.

The optimal product structure is to be able to rely only on the Blockchain when we want to store/read/verify data. Unfortunately while this book is being published we still need to rely on the government and other databases that aren’t on the Blockchain in the meanwhile so we can’t build our project in the optimal way, but we hope in the future this will be possible depending on the country regulations and progress towards using the Blockchain as a reliable technology.

Meanwhile our project structure is presented in Figure 4, we can see our features represented in the website, the connection we need to the Ethereum Blockchain using the METAMASK Wallet feature and the connection we need for the government database where we can verify the ownership of the asset and change the owner of the assets when a deal takes place in our website.



Evaluation/Verification Plan

Our evaluation and testing workspace is the Ropsten test network. Ropsten is a test blockchain where we can deploy our Smart Contract for free and test it before we upload it to the Ethereum Mainnet where we need to spend money doing it. Our testing will be divided into 2 sections Website testing and Smart Contract testing:

Website testing:

- **Testing the user registration for the website** - checking if the data is stored in the database. Checking if a user exits the website can log-in again. Checking that there won't be any duplication of users registered.
- **Testing the feature of creating a new NFT for the asset** - we need to check if the NFT created successfully in the Blockchain. We need to check if the website is able to detect if the user creating the NFT is the real owner of the asset that he wants to register using the government database. We need to check if NFT is added to the user assets list in the website.
- **Testing the search feature** – we need to check if the regular search and its filters work properly as expected.
- **Testing the bid feature** – testing if a user bids less than the published price of the asset then an error message needs to pop up. Testing if the request is transferred successfully for the seller and if the bid amount is correct. Testing if the request is added successfully to the seller request list and the seller can see it in his list.
- **Testing the assembling of the data that the website sends to the Smart Contract** – when a transaction between buyer and seller takes place the website needs to send the right data to the Smart Contract so it could make the transaction. So we need to check if the address of the buyer and seller are correct, we also need to check if the right amount of tax is calculated by using the government database.
- **Testing if the website is adapted to all devices** – testing the layout of the website in popular devices.
- **Testing the accept/decline request feature** – when a request is accepted we need to check if the transaction takes place successfully and every other request by other users is handled right by notifying them that the asset is sold.

Smart Contract Testing:

- **Testing if the Smart Contract is able to create an NFT** – when a request for creating a new NFT is delivered it must be created successfully with the right data and uploaded to the Blockchain.
- **Testing the ability of the Smart Contract to change the ownership of the NFT** - when a deal between the owner and the buyer takes place the smart contract needs to transfer the ownership of the NFT to the buyer's address.
- **Testing if the Smart Contract transfers the brokerage fee to our address** – when a transaction takes place a small percentage of the tokens transferred into our company's address.
- **Testing the Smart Contract basic functions** – when a basic function like balanceOf, ownerOf, and other basic functions operate when needed, we need to make sure they function as predicted.