



**COMILLAS**  
UNIVERSIDAD PONTIFICIA

ICAI

# GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

## APLICACIÓN DE USO DE BLOCKCHAIN Y CONTRATOS INTELIGENTES EN LA MULTIPROPIEDAD INMOBILIARIA

Autor: Alejandro Valbuena Núñez

Director: Atilano Fernández-Pacheco Sánchez-Migallón

Madrid



Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título  
Aplicación de uso de Blockchain y Contratos Inteligentes en la multipropiedad  
inmobiliaria

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico 2022/23 es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido

tomada de otros documentos está debidamente referenciada.



Fdo.: Alejandro Valbuena Núñez

Fecha: 4/7/ 2023

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

Fdo.: Atilano Fernández-Pacheco Sánchez-Migallón Fecha: ...../ ...../ .....





**COMILLAS**

UNIVERSIDAD PONTIFICIA

ICAI

# GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

## APLICACIÓN DE USO DE BLOCKCHAIN Y CONTRATOS INTELIGENTES EN LA MULTIPROPIEDAD INMOBILIARIA

Autor: Alejandro Valbuena Núñez

Director: Atilano Fernández-Pacheco Sánchez-Migallón

Madrid



# Agradecimientos

Quiero agradecer a mi familia, sobre todo a mis padres y a mi hermana que siempre me apoyan de manera incondicional, sobre todo en este último año que tan complicado ha sido a nivel personal y me han dado la oportunidad de llegar hasta aquí siendo una parte clave del proceso y no puedo describir lo agradecido que estoy hacia ellos.

A mis abuelos por ser mi ejemplo a seguir y por enseñarme a ver el lado bueno de las cosas y tener buena actitud por muy difícil que se ponga el camino.

Por último, agradecer a mi director de proyecto, Atilano, por darme la oportunidad de hacer este proyecto a pesar de los problemas que han surgido y encontrarnos a más de 7.000 kilómetros.



# **APLICACIÓN DE USO DE BLOCKCHAIN Y CONTRATOS INTELIGENTES EN LA MULTIPROPIEDAD INMOBILIARIA**

**Autor: Alejandro Valbuena Núñez.**

Director: Atilano Fernández-Pacheco Sánchez-Migallón.

Entidad Colaboradora: ICAI – Universidad Pontificia Comillas.

## **RESUMEN DEL PROYECTO**

Este Trabajo Fin de Grado ha consistido en el planteamiento y desarrollo de una DApp basada en la tecnología Blockchain que, mediante dos contratos inteligentes hace ver las posibilidades y beneficios que puede ofrecer este tipo de técnicas aplicadas al mercado inmobiliario. Este proyecto propone democratizar la compraventa de inmuebles para hacerla simple y accesible a todos los usuarios.

**Palabras clave:** Blockchain, Contratos Inteligentes, Inmuebles, Real Estate, token

## **1. Introducción**

Con la aparición de la tecnología Blockchain en 2008 y posteriormente las posibilidades que brindaron los Smart Contracts en 2014, se abrió una nueva ventana de oportunidades al mundo tecnológico. Con la capacidad de crear una red de manera descentralizada, que haga una gestión segura, pública e íntegra de los datos que se emplean en ella, los desarrolladores han tratado de buscar la aplicación práctica de ello en diversos ámbitos.

La evolución de la Blockchain ha dado lugar a las DApps o aplicaciones descentralizadas, las cuales permiten interactuar con la Blockchain por parte del usuario. Numerosos son los ejemplos de usos prácticos de esta tecnología en la industria, desde la gestión de documentación médica, como en el proyecto MedRec [1], desarrollado por investigadores del MIT que propone mejorar el acceso y gestión de datos médicos, hasta la trazabilidad en cadenas de producción como por ejemplo en el proyecto Food Trust [2], de IBM y Walmart.

Dada su inclusión en sectores muy variados, parece lógica su integración en el contexto del mercado inmobiliario, una de las formas de comercio y transmisión de valor más antiguas de la humanidad que sin embargo es siempre vista con cierto pesimismo y sensación de inaccesibilidad por el público general, sobre todo el público más joven.

Como se desarrolla en este proyecto, numerosas son las posibilidades que brinda el Blockchain al sector inmobiliario: su división en partes alícuotas para participar en rentabilidades generadas por el mismo como si de una empresa cotizada se tratase, la gestión de la gobernanza de una propiedad por múltiples propietarios a distancia, la propia compraventa segura con criptomonedas, entre otras. [3]

En este entorno se ubica el siguiente proyecto, hacerse valer de las soluciones Blockchain para crear una aplicación que permita la compraventa de activos inmobiliarios con criptomonedas con la supervisión de varios agentes que supervisen y validen la operación.

## **2. Definición del proyecto**

Con este Trabajo Fin de Grado se busca plantear y desarrollar un sistema descentralizado que implemente la flexibilidad que nos otorga la tecnología Blockchain en el sector inmobiliario, para ello se desarrollará una aplicación web que permita comprar y vender

inmuebles con la intervención de supervisores que validarán el proceso de compra para reforzar la seguridad del proceso.

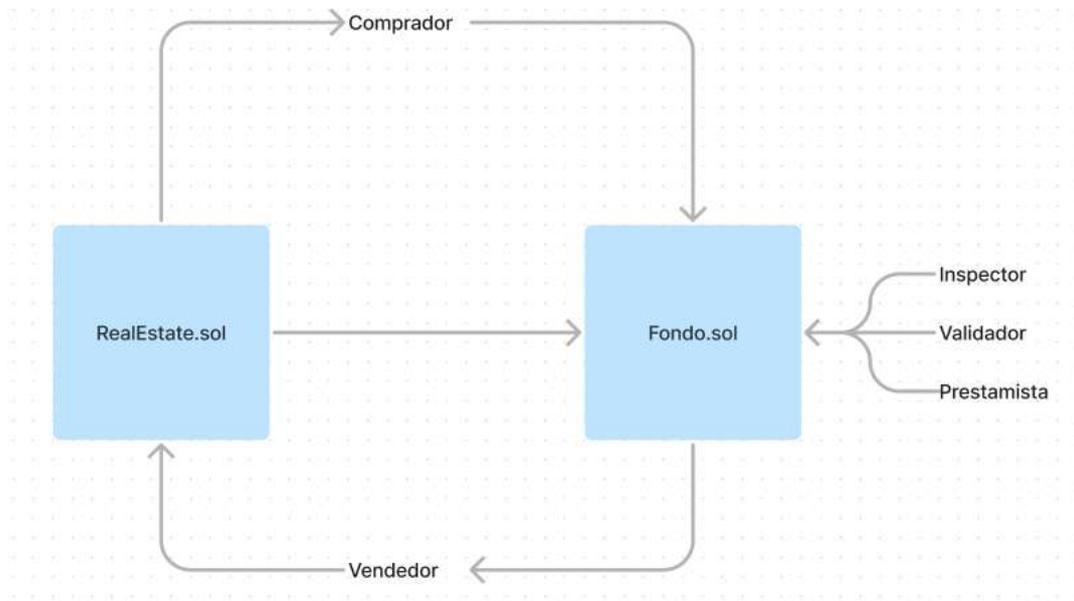
Se desarrollarán para este fin dos contratos inteligentes desplegados en Ethereum, el primero permitirá la creación de NFTs de bienes raíces digitales, así como su emisión y transferencia, mientras que el segundo será un depósito de garantía, el cual se utilizará para validar y facilitar la compraventa de dichos NFTs a través de sus funciones teniendo en cuenta la necesidad de supervisión para hacer el proceso completamente seguro. Ambos contratos se basan en el estándar de NFTs ERC721 y son desplegados y probados en una red Blockchain local.

La funcionalidad principal pues de este proyecto será la de transferir inmuebles entre usuarios de manera segura a través de la Blockchain.

### **3. Descripción del modelo/sistema/herramienta**

Como se ilustra en la imagen, la lógica del sistema se estructura alrededor de los dos Smart Contracts basados en Solidity. RealEstate.sol se encarga de crear los NFT y de identificarlos con un ID. Este contrato interactúa con el comprador cuando este decide adquirir un NFT y con el vendedor cuando por el contrario es el usuario el que desea vender su activo a través del contrato Fondo.sol, haciendo referencia al fondo de garantías. Este contrato se ha diseñado con la finalidad de aumentar lo máximo posible la seguridad y fiabilidad del sistema. Este contrato se encarga de retener el NFT y los fondos hasta que todos los participantes del proceso de venta den la aprobación a la misma. Este proceso se da de la siguiente manera: en primer lugar, el vendedor lista una propiedad para vender, cuando un comprador desea adquirirla, se retienen sus fondos mediante el fondo de garantía, posteriormente, el validador y el inspector aprueban la operación; cuando tiene el visto bueno de ambos, el prestamista aprueba también su

transacción y libera los fondos retenidos con anterioridad que son transmitidos a la cuenta vendedora y se transfiere la propiedad del NFT.



#### 4. Resultados

Los resultados del Trabajo Fin de Grado han sido satisfactorios. Se ha diseñado y desarrollado una aplicación web estética y funcional que permite la compraventa de NFT de bienes raíces mediante una cadena de bloques utilizando tecnologías actuales y de manera completamente funcional y operativa. En las figuras se observan la interfaz de la propia aplicación llamada Stalex y la interface de cada NFT donde se observa una foto del propio inmueble (generada por IA para este proyecto) y algunas de sus características y atributos principales.



Viviendas disponibles



**35 ETH**  
4 habitaciones | 2 baños | 320 m2  
Calle Ibiza, 31



**20 ETH**  
2 habitaciones | 2 baños | 240 m2  
Calle Hilarión Eslava, 31



**21 ETH**  
4 habitaciones | 2 baños | 400 m2  
Carrer del Mestral, Cambrils



**Madrid Retiro**

4 habitaciones | 2 baños | 320 m2  
Calle Ibiza, 31

**35 ETH**

Comprar

✕

---

**Resumen**

Precioso ático dúplex a 3 minutos del retiro

---

**Características**

- Precio de venta : 35
- Tipo de residencia : Apartamento
- Habitaciones : 4
- Baños : 2
- Metros cuadrados : 320
- Año de construcción : 1965

## 5. Conclusiones

En este Proyecto se han alcanzado los objetivos deseados al crear un mercado de bienes inmuebles alternativo haciéndose valer de la tecnología Blockchain y las criptomonedas. Se ha creado un sistema seguro y fiable para realizar la compraventa de bienes inmuebles de manera rápida y ágil.

Ha sido un reto el desarrollo del sistema al completo, sin embargo, el resultado es bueno y se estipulan ciertos caminos para su avance y siguientes pasos como la división en tokens de cada NFT inmueble o la posibilidad de incluir un sistema de gobernanza para

los mismos por parte de los poseedores de dichos tokens. A pesar de ello, el producto final cumple con lo esperado.

## **6. Referencias**

[1] MedRec, «Home,» [En línea]. Available: <https://medrec-m.com/>.

[2] IBM, «IBM Supply Chain Intelligence Suite: Food Trust,» [En línea]. Available: <https://www.ibm.com/es-es/products/supply-chain-intelligence-suite/food-trust>.

[3] M. Segura, «Tokenización de inmuebles: factores a tener en cuenta,» [En línea]. Available: <https://www.tokeniza.es/tokenizacion-de-inmuebles-factores-a-tener-en-cuenta/>.

# **APPLICATION OF BLOCKCHAIN AND SMART CONTRACTS USE IN REAL ESTATE TIMESHARING.**

**Author: Valbuena Núñez, Alejandro.**

Supervisor: Atilano Fernández-Pacheco Sánchez-Migallón.

Collaborating Entity: ICAI – Universidad Pontificia Comillas.

## **ABSTRACT**

This Final Degree Project has consisted in the proposal and development of a DApp based on Blockchain technology which, through two smart contracts, illustrates the possibilities and benefits that these techniques can offer when applied to the real estate market. This project aims to democratize the buying and selling of properties to make it simple and accessible to all users.

**Keywords:** Blockchain, Smart Contracts, Real Estate, token

## **1. Introduction**

With the emergence of Blockchain technology in 2008 and subsequently the possibilities offered by Smart Contracts in 2014, a new window of opportunities opened to the technological world. With the ability to create a network in a decentralized manner, that provides a secure, public, and integral management of the data used in it, developers have sought to find the practical application of it in various fields.

The evolution of Blockchain has given rise to DApps or decentralized applications, which allow user interaction with the Blockchain. Numerous are the examples of practical uses of this technology in the industry, from the management of medical documentation, as in the MedRec [1] project, developed by MIT researchers that proposes to improve the access and management of medical data, to traceability in production chains, for example, in the Food Trust project by IBM and Walmart. [2]

Given its inclusion in very varied sectors, its integration into the context of the real estate market seems logical. This is one of the oldest forms of commerce and value transfer in humanity, but it is always seen with some pessimism and a feeling of inaccessibility by the general public, especially the younger audience.

As developed in this project, there are numerous possibilities that Blockchain offers to the real estate sector: its division into aliquot parts to participate in returns generated by it as if it were a listed company, the management of the governance of a property by multiple distant owners, secure buying and selling with cryptocurrencies, among others. [3]

The following project is set in this environment, to take advantage of Blockchain solutions to create an application that allows the buying and selling of real estate assets with cryptocurrencies with the supervision of several agents who oversee and validate the operation.

## **2. Project's definition**

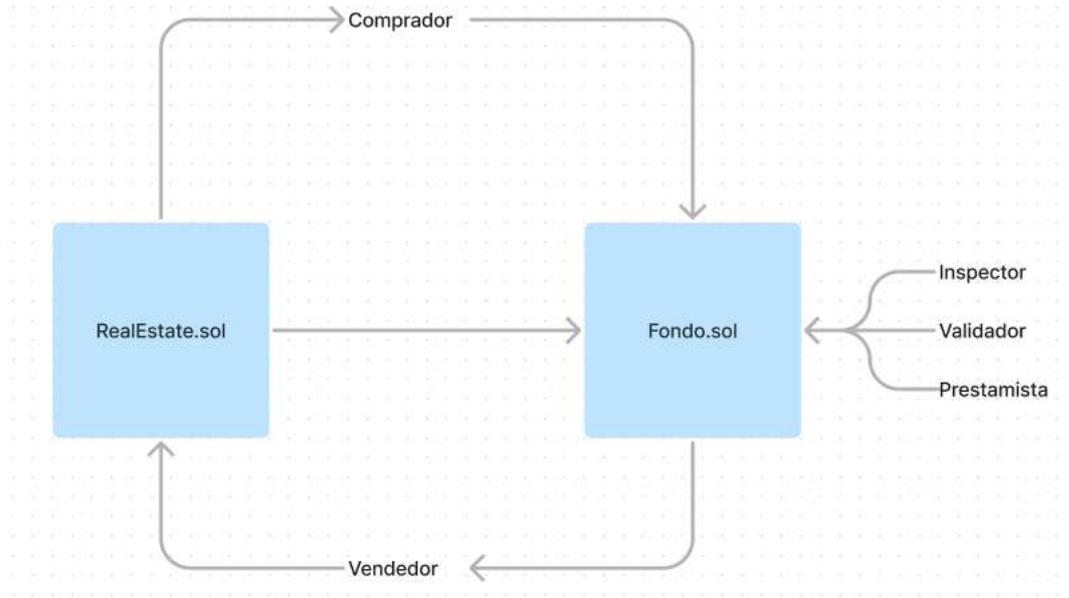
With this Final Degree Project, the objective is to propose and develop a decentralized system that leverages the flexibility and availability that blockchain technology offers in the real estate sector. To this end, a web application will be developed that enables the buying and selling of properties with the involvement of supervisors who will validate the purchasing process to reinforce the security of the operation.

Two smart contracts will be developed for this purpose, deployed on Ethereum. The first will allow for the creation of digital real estate NFTs as well as their issuance and transfer. Meanwhile, the second will act as an escrow, which will be used to validate and facilitate the buying and selling of these NFTs through its functions. Both contracts are based on the ERC721 NFT standard.

Therefore, the main functionality of this project is to securely transfer properties between users via the blockchain

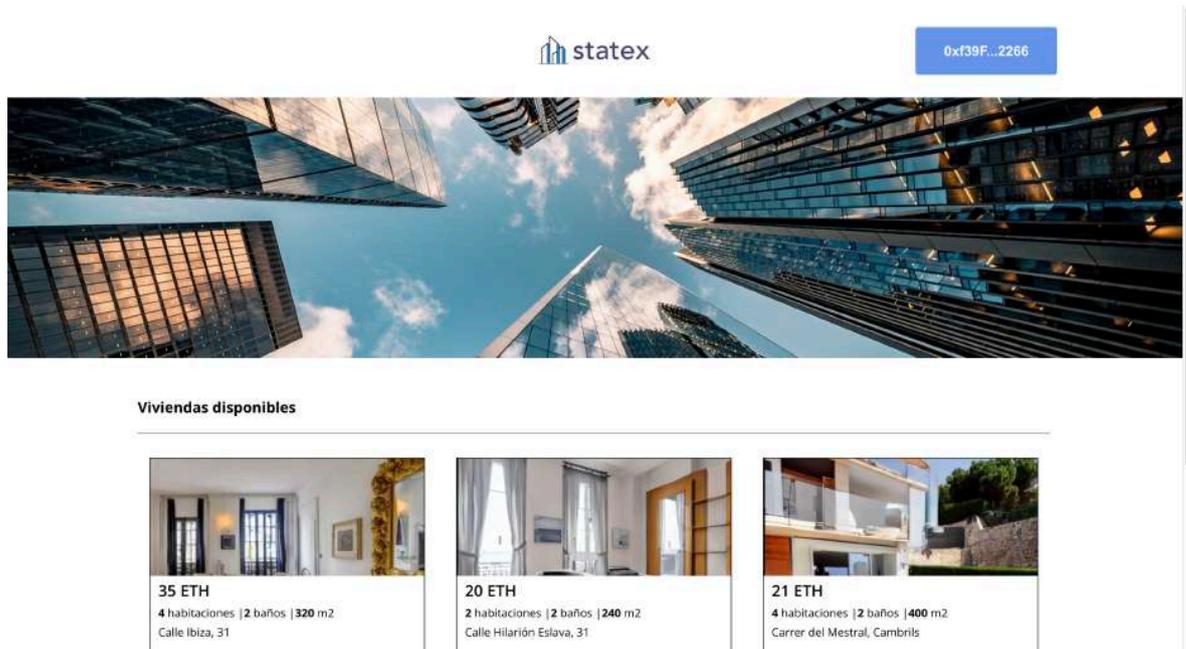
## **3. System's description**

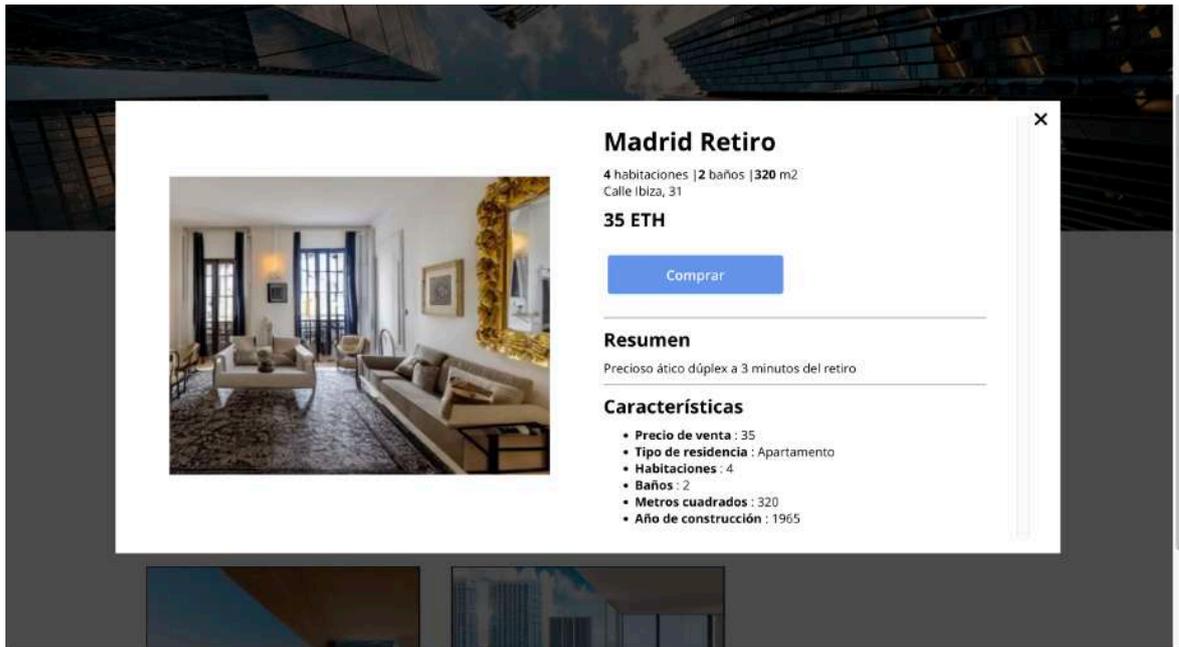
As illustrated in the image, the system logic is structured around two Solidity-based Smart Contracts. RealEstate.sol will be responsible for creating the NFTs and identifying them with an ID. This contract interacts with the buyer when they decide to acquire an NFT, and with the seller when, on the contrary, it's the user who wishes to sell their asset through the Fondo.sol contract, referring to the escrow fund. This contract is designed with the purpose of maximizing the security and reliability of the system as much as possible. This contract is responsible for holding the NFT and the funds until all participants in the sales process give their approval. This process occurs as follows: first, the seller lists a property for sale; when a buyer wishes to acquire it, their funds are held through the escrow fund. Subsequently, the validator and inspector approve the operation; when it has their approval, the lender also approves their transaction and releases the previously held funds, which are transferred to the seller's account, and the ownership of the NFT is transferred.



#### 4. Results

The results of the Final Degree Project have been satisfactory. An aesthetic and functional web application has been designed and developed that allows the buying and selling of real estate NFTs through a blockchain using current technologies in a fully functional and operational manner. The figures show the interface of the application itself, called Statex, and the interface of each NFT, where a photo of the property itself (generated by AI for this project) and some of its main characteristics and attributes can be seen.





## 5. Conclusion

In this Project, the desired objectives have been achieved by creating an alternative real estate market leveraging blockchain technology and cryptocurrencies. A secure and reliable system has been created to carry out the buying and selling of real estate in a quick and agile manner.

The full system development has been a challenge, however, the result is good and certain paths are stipulated for its advancement and next steps such as the tokenization of each real estate NFT or the possibility of including a governance system for them by the holders of said tokens. Despite this, the final product meets expectations.

## 6. References

[1] MedRec, «Home,» [En línea]. Available: <https://medrec-m.com/>.

[2] IBM, «IBM Supply Chain Intelligence Suite: Food Trust,» [En línea]. Available: <https://www.ibm.com/es-es/products/supply-chain-intelligence-suite/food-trust>.

[3] M. Segura, «Tokenización de inmuebles: factores a tener en cuenta,» [En línea].  
Available: <https://www.tokeniza.es/tokenizacion-de-inmuebles-factores-a-tener-en-cuenta/>.

## *Índice de la memoria*

<b>Capítulo 1. Introducción.....</b>	<b>6</b>
<b>Capítulo 2. Descripción de las Tecnologías .....</b>	<b>8</b>
2.1 Blockchain .....	8
2.2 Ethereum .....	9
2.3 smart contracts .....	9
2.3.1 Solidity.....	10
2.4 React .....	10
2.5 Node.js .....	11
2.6 npm .....	11
2.7 hardhat.....	11
2.8 OpenZeppelin.....	13
2.9 Metamask.....	13
2.10 Visual studio code.....	14
2.11 IPFS.....	15
2.12 Pinata.....	15
2.13 NFT .....	16
2.14 ERC721.....	16
<b>Capítulo 3. Estado de la Cuestión.....</b>	<b>18</b>
3.1 Blockchain .....	18
3.1.1 Criptografía .....	19
3.1.2 Direcciones .....	20
3.1.3 Contratos inteligentes .....	20
3.1.4 Bloques y cadena de bloques .....	21
3.1.5 Protocolos de consenso.....	22
3.1.6 Tokenización .....	23
3.2 El mercado inmobiliario actual.....	24
3.2.1 Proceso de compraventa actual.....	28
3.3 Proyectos blockchain inmobiliarios.....	29
<b>Capítulo 4. Definición del Trabajo.....</b>	<b>33</b>

4.1	Justificación .....	33
4.2	Objetivos .....	34
4.3	Metodología .....	34
4.4	Planificación y Estimación Económica.....	36
4.4.1	Costes materiales .....	36
4.4.2	Costes de desarrollo.....	38
4.4.3	Recursos humanos.....	39
4.4.4	Presupuesto total.....	39
<b>Capítulo 5.</b>	<b>Sistema/Modelo Desarrollado.....</b>	<b>43</b>
5.1	Diseño del sistema .....	43
5.1.1	Casos de Uso.....	46
5.2	Implementación.....	47
5.2.1	RealEstate.sol.....	47
5.2.2	Fondo.sol.....	49
5.2.3	IPFS.....	52
5.2.4	Hardhat .....	54
<b>Capítulo 6.</b>	<b>Análisis de Resultados .....</b>	<b>56</b>
<b>Capítulo 7.</b>	<b>Conclusiones y Trabajos Futuros.....</b>	<b>60</b>
<b>Capítulo 8.</b>	<b>Bibliografía.....</b>	<b>63</b>
<b>ANEXO I:</b>	<b>ALINEACIÓN DEL PROYECTO CON LOS ODS.....</b>	<b>69</b>
<b>ANEXO II:</b>	<b>Manual de usuario .....</b>	<b>71</b>
<b>ANEXO III:</b>	<b>Manual de instalación.....</b>	<b>75</b>

## *Índice de figuras*

Figura 1 - Logo de Ethereum (Fuente: New Atlas).....	9
Figura 2 - Código ejemplo Solidity.....	10
Figura 3 - Ejemplo de Hardhat para crear una Blockchain local .....	12
Figura 4 – Metamask.....	14
Figura 5 - Descripción gráfica de una cadena de bloques (Fuente: Cortesía de ResearchGate) .....	22
Figura 6 - Principal diferencia entre los dos protocolos de consenso más importantes (Fuente: Cortesía de Patika Academy) .....	23
Figura 7 - Compraventa de viviendas en España (Fuente: Cortesía de KPMG) [31] .....	26
Figura 8 - Evolución del número de transacciones inmobiliarias de viviendas en España por trimestre (Fuente: Elaboración propia, con datos del Ministerio) [47].....	40
Figura 9 - Cálculo de los beneficios brutos anuales.....	41
Figura 10 - Ingresos brutos estimados caso menos favorable.....	42
Figura 11 - Flujo del diseño (Elaboración propia) .....	44
Figura 12 - Diseño de la lógica del sistema (elaboración propia).....	45
Figura 13 - Proceso de compra.....	46
Figura 14 - Código fuente del contrato RealEstate.sol.....	47
Figura 15 - Código contrato Fondo.sol .....	51
Figura 16 - JSON con la información de cada inmueble .....	53
Figura 17 - Interfaz de usuario de Pinata .....	54
Figura 18 - Fichero con información de los inmuebles subido a IPFS .....	54
Figura 19 - Fichero con las imágenes subido a IPFS .....	54
Figura 20 - Test contrato Fondo.sol .....	57
Figura 21 - Aspecto final aplicación .....	57
Figura 22 - Aspecto inmuebles listados .....	58
Figura 23 - Pruebas transacciones.....	59

---

Figura 24 - ODS. Fuente: ONU .....	69
Figura 25 - Statex sin conectar la cartera .....	71
Figura 26 - Apariencia de usuario con la cartera conectada .....	72
Figura 27 - Apartado viviendas disponibles Statex.....	72
Figura 28 - Ejemplo de inmueble listado .....	73
Figura 29 - Transacción ejemplo.....	74
Figura 30 - Venta aprobada.....	74
Figura 31 - Instalación Node.js .....	75
Figura 32 - Instalación de VS Code .....	76
Figura 33 - Abrir terminal VS Code .....	76
Figura 34 - Nueva terminal .....	77

## *Índice de tablas*

Tabla 1 - Función Hash SHA-256.....	19
Tabla 2 - Diagrama de Gant del proyecto .....	35
Tabla 3 - Características técnicas ordenador portátil .....	36
Tabla 4 - Especificaciones Monitor .....	37
Tabla 5 - Distribución de las horas.....	38
Tabla 6 - Resumen de los costes de desarrollo.....	39

## Capítulo 1. INTRODUCCIÓN

En el último cuarto de siglo, la humanidad ha presenciado uno de los mayores cambios en su historia, debido a las nuevas tecnologías, que ha trascendido en todos los aspectos de la vida. Desde lo más cotidiano como hacer la compra hasta sofisticadas cadenas de producción tan complejas como la de un avión comercial se han visto adaptadas y mejoradas por los avances tecnológicos de esta nueva sociedad moderna. [1]

Sin embargo, el que probablemente haya sido el gran hito de la historia moderna es el desarrollo e implementación masiva del internet en todos los ámbitos de la vida y las relaciones humanas ya que esto ha redefinido la forma de vivir e interactuar entre sí y con el medio. Internet ha conectado a las personas, entidades y países como nunca podría haberse imaginado, y ha democratizado procesos que antes estaban únicamente al alcance de unos pocos. Por ejemplo, el proceso de comprar o vender una acción bursátil, hace 50 años era una tarea mucho más tediosa de lo que es ahora, había que personarse físicamente en la Bolsa donde operase la empresa de la que se quería obtener una acción y realizar la operación a través de un bróker e incluso había que guardar el título físico. Esto, a un inversor actual que puede operar cualquier bolsa desde cualquier lugar del mundo simplemente con una conexión a internet y un dispositivo que acceda a ello, le haría muy probablemente replantearse su voluntad de invertir en el mercado de valores. [1]

Con el nacimiento en el año 2008 de la mano de Satoshi Nakamoto y su *paper: Bitcoin: A Peer-to-Peer Electronic Cash System* [2] del concepto Blockchain, un nuevo abanico de oportunidades se abrió a los desarrolladores, que pudieron ver como esta tecnología les permitía resolver grandes problemas a la hora de dar credibilidad a un sistema susceptible de ser alterado o corrompido pues almacena los datos de transacciones entre dos o más partes de forma descentralizada y distribuida y sin intermediarios de manera segura inmutable e íntegra.

En 2014, el mundo Blockchain vio sus posibilidades disparadas cuando Vitalik Buterin publicó el *paper: Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform* que dio vida al Blockchain 2.0, introduciendo los Smart Contracts en la Blockchain. [3]

En este punto, este tipo de tecnología evolucionó, surgiendo las aplicaciones descentralizadas o DApps, que permitían el alojamiento de la aplicación de manera descentralizada en la Blockchain dando así una utilidad mucho mayor para usuarios y empresas finales.

Con este Trabajo Fin de Grado, se intenta poner en contexto el cómo se ha adaptado el mercado inmobiliario a las nuevas herramientas y tecnologías disponibles mediante un caso de uso de una posible solución de aplicación descentralizada que gestiona la creación de los Smart Contracts de los bienes raíces, así como su compraventa y la gestión de la multipropiedad de los mismos.

Pese a que en el mercado existen diferentes soluciones, no hay un verdadero referente en este sector que históricamente ha sido uno de los más lucrativos para los grandes inversores, ya sea porque las propuestas que existen actualmente son poco atractivas o difíciles de usar para el usuario final. Sin embargo, si se diesen las condiciones óptimas y resultase un producto final atractivo para el mercado, se produciría una revolución total en este sector ya que sería muy fácil gestionar propiedades como si de acciones de una sociedad se tratasen de una manera segura e incorruptible dando acceso a un perfil de inversor mucho más cotidiano que puede participar con menos capital. [4]

Este es, en resumidas cuentas, el propósito final de la tecnología en nuestra sociedad, facilitar las conexiones humanas, ya sea con fines mercantiles o sociales y acabar con barreras y dificultades de todo tipo, de capital, geográficas, de conocimiento o de forma y acercar el mundo financiero e inversor a la mayor cantidad de personas, haciendo crecer así la economía y las oportunidades.

## Capítulo 2. DESCRIPCIÓN DE LAS TECNOLOGÍAS

A continuación, se describirán las principales tecnologías y servicios utilizados en el desarrollo de este proyecto, así como Blockchain, Ethereum, Nodejs entre otros.

### 2.1 BLOCKCHAIN

Blockchain fue por primera vez definido e introducido en el 2008, en el *paper* de Satoshi Nakamoto llamado “Bitcoin: Un Sistema de Efectivo Electrónico Usuario-a-Usuario” donde se describía una red de pagos online de forma descentralizada, segura e independiente llamada Bitcoin. Esta fue la primera red Blockchain, en adelante este primer tipo se denomina Blockchain 1.0. [2]

Según el Banco Santander [5], Blockchain es *una base de datos compartida o distribuida donde la información registrada está almacenada en bloques, ligados entre sí criptográficamente, y validada de una forma descentralizada a través de un protocolo común*. Así pues, se define Blockchain como una red segura prácticamente imposible de manipular. La única forma de que un tercero modificase los datos de una Blockchain a su antojo sería mediante un ataque del 51%, donde dicho atacante tendría el control del 51% de los nodos que forman la cadena de forma que podría manipular el protocolo de consenso e introducir información maliciosa. En la práctica, en redes establecidas como Ethereum que cuenta con más de 500.000 validadores o Bitcoin que requeriría una cantidad de energía desmesurada, es algo casi imposible de conseguir. [6]

Una de las características más potentes de Blockchain es la descentralización, es decir, la capacidad de operar sin la necesidad de una empresa o entidad central que la regule y gobierne, se trata pues de una red usuario-usuario que muy difícilmente puede ser manipulada. [7]

## **2.2 ETHEREUM**

La plataforma lanzada en 2015 Ethereum proponía una mejora respecto a Bitcoin yendo más allá y permitiendo ejecutar código en su red, con ello nacen los contratos inteligentes y las aplicaciones descentralizadas, los cuales abren un nuevo camino en la historia de la tecnología Blockchain, dando lugar a la llamada Blockchain 2.0. [3]

La versatilidad que proporciona Ethereum a los desarrolladores ha hecho que crezca con una gran velocidad, posicionándose como el segundo proyecto basado en Blockchain más grande y con mayor capital detrás del mundo, alcanzando su token nativo una capitalización de mercado de 559.91 miles de millones de dólares americanos en octubre de 2021.<sup>1</sup>



*Figura 1 - Logo de Ethereum (Fuente: New Atlas)*

## **2.3 SMART CONTRACTS**

Los Smart Contracts o contratos inteligentes, son programas autónomos que corren en la Blockchain y se ejecutan de forma automática cuando se reúnen las características acordadas en el mismo. Estos Smart Contracts en la aplicación desarrollada están programados en Solidity. [8]

---

<sup>1</sup> Datos de cotización: <https://coinmarketcap.com/currencies/ethereum/>

### 2.3.1 SOLIDITY

Se trata de un lenguaje de programación de alto nivel orientado a objetos enfocado en la creación de contratos inteligentes utilizado en diversas Blockchain compatibles con este tipo de tecnologías. [9]

A continuación, se muestra un breve ejemplo de un contador en Solidity:

```
pragma solidity ^0.8.0;

contract Contador {
    uint256 public count;

    constructor() {
        count = 0;
    }

    function aumentar() public {
        count++;
    }

    function disminuir() public {
        count--;
    }
}
```

*Figura 2 - Código ejemplo Solidity*

## 2.4 REACT

React se trata de una biblioteca JavaScript de código abierto desarrollada por Facebook que se emplea en la programación de aplicaciones web para crear interfaces de usuario interactivas. React divide la interfaz de usuario en bloques autónomos con el fin de poder reutilizarse y combinarse manteniendo su lógica propia. Esta estrategia de compartimentalización ha posicionado a React como una opción muy buscada al diseñar aplicaciones de una sola página que demandan actualizaciones rápidas y fluidas. [9]

En este proyecto se ha utilizado React dada su eficiencia y rendimiento aparte de la compatibilidad con librerías muy convenientes para el desarrollo del proyecto.

## **2.5** *NODE.JS*

Node.js es un entorno de ejecución de JavaScript creado sobre el motor JavaScript V8 de Google Chrome. Se concibió inicialmente para facilitar la creación de aplicaciones de red escalables, y desde entonces se ha expandido para cubrir una multitud de casos de uso, desde la construcción de APIs hasta la creación de soluciones completas de back-end. [11]

Node.js funciona utilizando un modelo de E/S (entrada/salida) asíncrono basado en eventos. Este modelo permite que Node.js maneje múltiples solicitudes de manera concurrente sin bloquear el flujo de ejecución. Es esencialmente un bucle de eventos que escucha solicitudes y luego las despacha a través de devoluciones de llamada, permitiendo que múltiples operaciones se realicen simultáneamente sin la necesidad de hilos adicionales. [11]

Este enfoque de Node.js le permite manejar un gran número de solicitudes simultáneas con alta eficiencia, lo que lo convierte en una excelente opción para aplicaciones web en tiempo real y de alto rendimiento. Al mismo tiempo, debido a que JavaScript se utiliza tanto en el cliente como en el servidor, se facilita un entorno de desarrollo uniforme, que puede mejorar la productividad y el rendimiento del equipo de desarrollo.

## **2.6** *NPM*

Se trata de un gestor de paquetes que es el utilizado por Node.js por defecto. Es un software gratuito y compatible con los principales sistemas operativos del mercado. [12]

Se ha utilizado en este proyecto para el despliegue de los archivos para la interfaz web y el servidor.

## **2.7** *HARDHAT*

Hardhat es un entorno de desarrollo de Ethereum que se utiliza en la programación de aplicaciones web descentralizadas basadas en la cadena de bloques de Ethereum. Hardhat

facilita herramientas para desarrollar, compilar, desplegar y probar contratos inteligentes de manera eficiente desde la terminal o desde el entorno de desarrollo. [13]

En este proyecto se ha utilizado Hardhat para generar una Blockchain local con carteras de prueba para poder comprobar que los contratos funcionan correctamente y que la página se conecta sin problemas a la Blockchain.

En la Figura 3 podemos ver la utilización del comando node para generar 10 carteras de prueba cada una con su dirección y 10000 ETH perfectamente funcionales y disponibles a través de Metamask.

Asimismo, también se ha utilizado Hardhat para lanzar los contratos en la red.

```
(base) alejandrovalbuena@MacBook-Pro-de-Alejandro statex % npx hardhat node
Started HTTP and WebSocket JSON-RPC server at http://127.0.0.1:8545/

Accounts
=====

WARNING: These accounts, and their private keys, are publicly known.
Any funds sent to them on Mainnet or any other live network WILL BE LOST.

Account #0: 0xf39Fd6e51aad88F6F4ce6aB8827279cFfFb92266 (10000 ETH)
Private Key: 0xac0974bec39a17e36ba4a6b4d238ff944bacb478cbed5efcae784d7bf4f2ff80

Account #1: 0x70997970C51812dc3A010C7d01b50e0d17dc79C8 (10000 ETH)
Private Key: 0x59c6995e998f97a5a0044966f0945389dc9e86dae88c7a8412f4603b6b78690d

Account #2: 0x3C44CdDdB6a900fa2b585dd299e03d12FA4293BC (10000 ETH)
Private Key: 0x5de4111afa1a4b94908f83103eb1f1706367c2e68ca870fc3fb9a804cdab365a

Account #3: 0x90F79bf6EB2c4f870365E785982E1f101E93b906 (10000 ETH)
Private Key: 0x7c852118294e51e653712a81e05800f419141751be58f605c371e15141b007a6

Account #4: 0x15d34AAf54267DB7D7c367839AAf71A00a2C6A65 (10000 ETH)
Private Key: 0x47e179ec197488593b187f80a00eb0da91f1b9d0b13f8733639f19c30a34926a
```

*Figura 3 - Ejemplo de Hardhat para crear una Blockchain local*

## **2.8 OPENZEPPELIN**

OpenZeppelin se comporta como un libro de referencia para la creación de contratos inteligentes seguros en Ethereum y otras redes Blockchain que son compatibles con la Máquina Virtual de Ethereum (EVM). Su objetivo principal es asistir a los desarrolladores en la construcción de contratos inteligentes de manera eficaz y segura, minimizando así la probabilidad de errores y brechas de seguridad. [14]

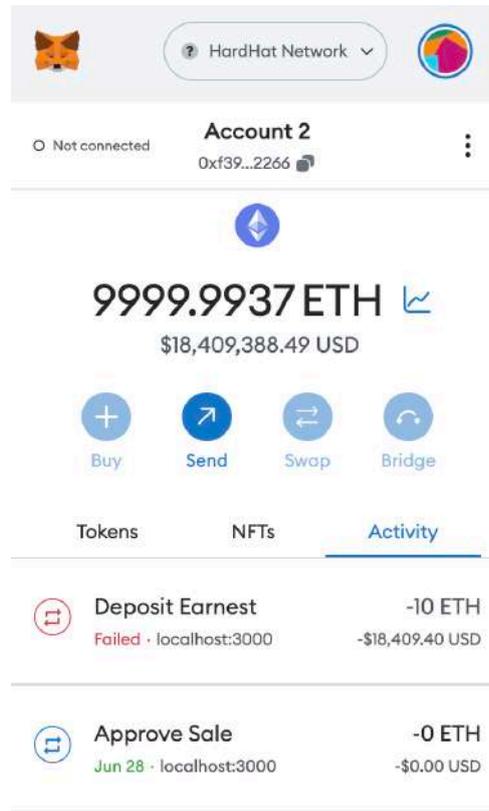
La librería OpenZeppelin aporta aplicaciones de estándares de contratos inteligentes, como ERC20 y ERC721, este último ha sido utilizado en el desarrollo, los cuales han obtenido una amplia aceptación y uso en la comunidad. Al aprovechar estas implementaciones ya existentes, los desarrolladores pueden economizar tiempo y evitar problemas de seguridad, evitando la necesidad de redactar estos contratos desde cero. [14]

OpenZeppelin también provee características extra como cálculos matemáticos seguros, manejo de permisos basado en roles, y un entorno para contratos actualizables. Estos contratos son sometidos a auditorías por parte del equipo de OpenZeppelin, ayudando a garantizar su seguridad y la ausencia de vulnerabilidades conocidas.

## **2.9 METAMASK**

Metamask es una cartera de criptomonedas compatible con las redes Blockchain y aplicaciones descentralizadas basadas en Ethereum. Metamask se instala como una extensión de Google Chrome y permite al usuario custodiar sus criptoactivos en un entorno seguro.

Además de funcionar como cartera, Metamask permite interactuar con las aplicaciones descentralizadas basadas en Ethereum conectándose a ellas de manera muy sencilla e intuitiva. Metamask simplifica también el proceso de firma y confirmación de las transacciones que se dan en la Blockchain. En la Figura 4 se puede ver un ejemplo de Metamask en el navegador. [15]



*Figura 4 – Metamask*

## ***2.10 VISUAL STUDIO CODE***

Se trata del editor de código *open source* de Microsoft. Es uno de los editores más usados por los programadores por su disponibilidad en Linux, Windows y macOS, su apariencia agradable, la posibilidad de ejecutar comandos en la terminal desde el propio editor, su integración con GitHub y las múltiples extensiones disponibles que hacen la programación más fácil. Visual Studio Code ha sido el editor de código empleado en este proyecto por su velocidad de ejecución y versatilidad. [16]

## ***2.11 IPFS***

IPFS (InterPlanetary File System) es un protocolo de distribución de archivos *peer-to-peer* que permite distribuir y acceder de manera descentralizada y distribuida a contenido en la web. IPFS fue desarrollado por Juan Benet en 2015 como intento de reemplazar el protocolo HTTP (Hyper Text Transfer Protocol) y hacerlo más seguro y eficiente. Cada archivo tiene una huella única en la cadena denominado hash. [17]

El objetivo principal de IPFS es solventar la falta de descentralización y de permanencia en la web existente, por ello distribuye la información en múltiples nodos en lugar de guardarla en un servidor centralizado evitando la censura y la disponibilidad de contenido en la medida de lo posible además de reducir la infraestructura costosa, compleja y vulnerable que estos servidores conllevan. [17]

En este proyecto, se ha empleado IPFS para la creación de NFTs, guardando la información de los inmuebles en archivos JSON subidos a IPFS.

## ***2.12 PINATA***

Pinata es un servicio en la nube utilizado para facilitar la interacción con la IPFS. Pinata simplifica el proceso de almacenamiento y administración de archivos en IPFS al proporcionar una interfaz gráfica intuitiva y fácil de usar, junto con una serie de poderosas funciones de API para integrar IPFS en sus propias aplicaciones. [18]

A través de Pinata, se puede subir, alojar y administrar contenido en IPFS de manera muy simple. El servicio actúa como un intermediario con la red IPFS, facilitando las operaciones y aliviando a los usuarios de la necesidad de configurar y mantener su propio nodo IPFS. [18]

En este proyecto, Pinata ha sido empleado para el almacenamiento de información inmobiliaria. Se ha utilizado para subir a la red IPFS los detalles de las propiedades, incluyendo datos como la ubicación, tamaño, precio y más. Además, se ha aprovechado para

almacenar imágenes de las propiedades, proporcionando un sistema eficiente y descentralizado para el almacenamiento de estos recursos visuales importantes. Esta información ha sido guardada en formato JSON en la red IPFS con la información de cada NFT.

### ***2.13 NFT***

Los NFTs, o Tokens No Fungibles, son una clase especial de tokens criptográficos que representan algo único. A diferencia de las criptomonedas tradicionales como Bitcoin o Ethereum, que son intercambiables, los NFTs no lo son debido a su individualidad intrínseca. Cada NFT tiene un valor y atributos específicos que son únicos para ese token, lo que significa que no puede ser reemplazado con otro token idéntico. [19]

Los NFTs pueden ser utilizados para demostrar la propiedad digital de una amplia gama de bienes tangibles e intangibles. Esto puede ir desde obras de arte hasta propiedades virtuales en videojuegos e incluso derechos de autor. La capacidad de los NFTs de autenticar y verificar la propiedad es una de sus características más atractivas y explicativas de su creciente popularidad. [19]

Las características comentadas hacen a los NFTs una tecnología idónea para el objetivo del proyecto en cuestión.

### ***2.14 ERC721***

El estándar ERC721 en la Blockchain Ethereum establece las bases para la creación y manipulación de tokens no fungibles. Este estándar es de gran utilidad para los desarrolladores que desean construir y manejar tokens no fungibles de manera optimizada en la red Ethereum. [20]

Su aplicación se extiende a una variedad de áreas, incluyendo la creación de arte digital, propiedad virtual en juegos y la gestión de coleccionables digitales, entre otros.

ERC721 es importante dada su facilitación de la interoperabilidad entre diversas interfaces contractuales para los NFTs. Esto implica que un único contrato inteligente puede tener la capacidad de administrar, transferir y gestionar múltiples tokens únicos. [20]

## **Capítulo 3. ESTADO DE LA CUESTIÓN**

Se desarrollará el contexto del trabajo, prestando atención a la tecnología Blockchain en la que se basa y al mercado inmobiliario, así como las distintas soluciones existentes en línea con la propuesta.

### **3.1 BLOCKCHAIN**

La tecnología Blockchain ha sido uno de los temas más populares en los últimos años. Ya sea por su implicación en el mundo de las criptomonedas o por el abanico de posibilidades que brinda con aplicaciones de todo tipo.

En 2021, tras la pandemia de COVID-19, ante un escenario de incertidumbre y especulación en los mercados globales, las criptomonedas y otros activos criptográficos como los NFT tuvieron un gran auge global, contemplándose subidas en los precios de algunos activos como el Bitcoin, que vio su valor aumentado entre marzo de 2020 y noviembre de 2021 en un 1200%. Con el tiempo, el valor de estos activos se ha normalizado, y muchos proyectos de criptomonedas carentes de un propósito y modelo de negocio sólido, han desaparecido trayendo consigo pérdidas importantes para aquellos que decidieron confiar en ellos. A pesar del mal resultado para algunos, durante los primeros meses de 2021 era uno de los principales temas de conversación del momento, según Google Trends, los términos Bitcoin y Blockchain experimentaron varios de sus máximos relativos históricos de popularidad en este periodo poniendo a la tecnología en el mapa.<sup>2</sup>

En la actualidad, este tipo de tecnología tiene una cantidad de aplicaciones cada vez mayor en ámbitos muy variados, destacando, por ejemplo, el uso que le da la empresa MedRec [1], que propone un sistema para compartir historias médicas y datos sensibles sobre

---

<sup>2</sup> [1] Google trends, <https://trends.google.com/home> (accessed Jul. 4, 2023).

medicamentos de forma segura e incorruptible debido a las características propias de Blockchain.

Se van a explicar los principales componentes de una red Blockchain.

### 3.1.1 CRIPTOGRAFÍA

Dos de las características más importantes de la Blockchain es que es una tecnología segura que garantiza la integridad de los datos, para ello implementa las funciones hash criptográficas. Este tipo de funciones, encriptan el input que reciben de manera que dos datos iguales a los que se les aplica la misma función producirán el mismo hash, sin embargo, cualquier mínimo cambio, aunque sea a nivel de bit, generará un hash radicalmente distinto.

En la Tabla 1, se observa el resultado de aplicar la función SHA-256 (la más usada) a tres valores distintos. Se observa como el simple cambio de una letra de mayúsculas a minúsculas genera un output completamente distinto. [23]

<i>Texto input</i>	<i>Output (SHA-256)</i>
Hello World	a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e
Blockchain	625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1
blockchain	ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1

*Tabla 1 - Función Hash SHA-256*

Por la definición de una función hash, esta debe ser [24]:

- Resistente a preimágenes, es decir, es difícil encontrar una entrada dada una salida.
- Segunda resistencia a preimágenes, es decir, que no sea fácil encontrar una entrada con la misma salida que otra distinta.
- Resistente a colisiones, es decir, no es fácil encontrar dos entradas distintas con la misma salida.

Cada bloque de la cadena cuenta con un hash asociado calculado a partir de los datos de sí mismo y el hash del bloque inmediatamente anterior.

### **3.1.2 DIRECCIONES**

Existen una gran cantidad de redes Blockchain que utilizan direcciones internas, por ejemplo, todas las que permiten las transferencias de criptomonedas como Ethereum cuentan con direcciones de cartera únicas, calculadas de diferentes maneras dependiendo la red en la que nos encontremos, normalmente aplicando una función hash [25]. Un ejemplo de una dirección de cartera Ethereum:

0xC2b9166867660AF5C07dD70670D5B6B0021e8BF9

Estas direcciones, se pueden comparar con cuentas bancarias en el mundo analógico y es una especie de identificación personal dentro de la cadena de bloques, algo que hace al usuario único y le dota de identidad.

Las direcciones de cartera también permiten un cierto nivel de privacidad para los usuarios. Aunque las transacciones son públicas y rastreables, no revelan la identidad real del usuario, sólo su dirección de cartera. De esta manera, se puede mantener la confidencialidad al realizar transacciones.

### **3.1.3 CONTRATOS INTELIGENTES**

Los contratos inteligentes son programas informáticos que facilitan, verifican y ejecutan un contrato digital de manera autónoma. Se trata de programas autoejecutables, por lo que eliminan los intermediarios y terceros en los que confiar, simplemente se cumplen siempre que se den las condiciones establecidas. [26]

Los contratos inteligentes dependiendo de la red en la que se alojen se programan en diferentes lenguajes de programación, desde Solidity en el caso de la red Ethereum (aunque también se pueden realizar con Vyper) hasta lenguajes menos conocidos como Rust, Ride, Cairo o incluso C++ [27].

La aplicación y potencial de estos contratos es inmensa, hasta el punto de cuestionar y revolucionar la forma en la que muchos negocios hacen industria. En el contexto de este proyecto, los contratos inteligentes aplicados al sector de los bienes raíces pueden ser utilizados para resolver las transacciones inmobiliarias de forma eficiente y segura, para gestionar contratos de arrendamientos automatizando el cobro de la renta o incluso para tokenizar propiedades donde múltiples inversores cuentan con fracciones de la misma.

Una de las aplicaciones más comunes de los contratos inteligentes es la creación de tokens no fungibles o NFT. [26]

### **3.1.4 BLOQUES Y CADENA DE BLOQUES**

Los bloques, como su propio nombre indica, son la estructura principal de la Blockchain, conforman su columna vertebral representando un conjunto de transacciones encapsuladas que son validadas y publicadas a la red Blockchain de forma conjunta. Cada bloque está vinculado con su anterior y el siguiente, creando así una cadena de bloques. [7]

Cada bloque cuenta con su propia cabecera donde se almacenan los metadatos del mismo que aseguran la integridad y su correcto funcionamiento. En esta cabecera se incluye el hash de la cabecera anterior y el hash de los datos del bloque, combinándose así y creando un bloque completamente único. [7]

La Figura 5 ofrece una representación gráfica de la estructura de un bloque y su contenido. En ella se puede observar cómo el bloque N mantiene la información del hash tanto del bloque N como del bloque N-1. Así, los bloques se encuentran interconectados de tal manera que cualquier intento de introducir un bloque alterado en la red sería detectado de inmediato. Esta capacidad de detección se debe a que un bloque manipulado no contendría la información hash correcta y, por lo tanto, sería identificado y eliminado por los nodos de la red.

Esta estructura de bloques facilita el registro seguro y transparente de las transacciones, de forma robusta y confiable.

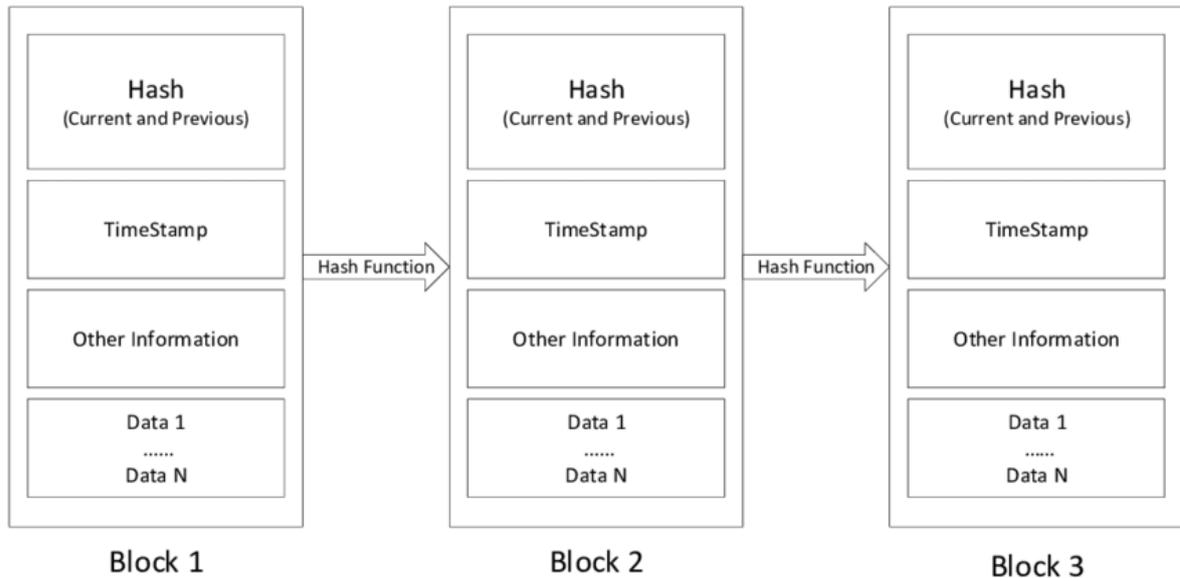


Figura 5 - Descripción gráfica de una cadena de bloques (Fuente: Cortesía de ResearchGate)

### 3.1.5 PROTOCOLOS DE CONSENSO

Una parte crucial de una red Blockchain son los protocolos de consenso o protocolos de validación, mediante los cuales, los nodos llegan a un acuerdo sobre la seguridad y la integridad de la cadena. Existen diversos protocolos, cada red se estructura en torno a uno de ellos, algunos de los más importantes se exponen a continuación [28]:

- **Proof of work (PoW):** en este tipo de protocolos, los nodos, (también conocidos como mineros) compiten entre sí para resolver un complejo problema criptográfico, el primero en hacerlo, agrega el nuevo bloque a la cadena y a cambio recibe una recompensa. De esta forma, mediante la realización de una actividad genuina, muy costosa a nivel computacional se garantiza la seguridad de la red. Este protocolo es utilizado por redes como Bitcoin.
- **Proof of Stake (PoS):** en este protocolo, a partir de tener cierta importancia relativa en la red, se puede participar en ella como validador de nuevos bloques. Cuánto más importante sea un nodo dentro de la red, mayor será la probabilidad de este de ser elegido para agregar un nuevo bloque, este bloque deberá de ser supervisado por el

resto de los nodos y si todo es correcto, se añadirá correctamente al final de la cadena. Cuando un nodo es elegido para añadir un bloque, sus monedas son bloqueadas por la red. Si el bloque es correcto y finalmente válido, se desbloquean añadiendo una compensación. De esta manera se incentiva la seguridad y buen funcionamiento de la Blockchain consumiendo menos energía y poder computacional que PoW. Entre otras, este es el protocolo que utiliza la red Ethereum. En la Figura 6 se puede ver la diferencia entre PoW y PoS de manera abstracta y visual.

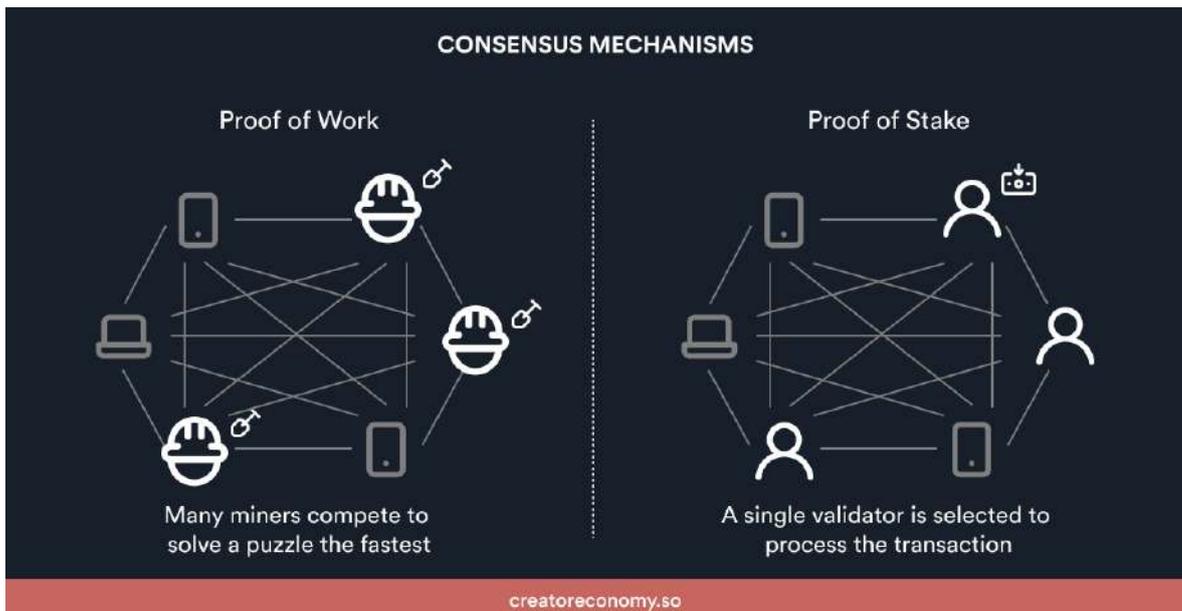


Figura 6 - Principal diferencia entre los dos protocolos de consenso más importantes (Fuente: Cortesía de Patika Academy)

- Existen otros mecanismos de validación, mucho menos usados que los dos anteriores, como por ejemplo DPoS (Delegated Proof of Stake) y PBFT (Practical Byzantine Fault Tolerance) donde se utilizan criterios propios de la descentralización y la resistencia a fallos.

### 3.1.6 TOKENIZACIÓN

A través de la tokenización, un objeto tangible o un derecho sobre un activo se puede convertir en un representante digital en la cadena de bloques, el cual es seguro, auditable y

transferible en todo el mundo. Esto se traduce en una mayor liquidez y accesibilidad para los activos, y permite a los propietarios potencialmente llegar a una base de inversores mucho más amplia. [3]

Además de los beneficios de liquidez y accesibilidad, la tokenización también aporta transparencia al proceso. La naturaleza de la cadena de bloques garantiza que cada transacción y cambio de propiedad del token esté registrada y sea fácil de rastrear, proporcionando una mayor confianza en la propiedad. [29]

Este nuevo método de representación de la propiedad de los activos también está permitiendo nuevas formas de interacción y comercialización. Como ejemplo, podemos citar el reciente auge de los tokens no fungibles o NFTs en el mundo del arte y los coleccionables. Con los NFTs, los artistas pueden tokenizar su trabajo, otorgándoles una única representación digital que puede ser vendida o intercambiada. Esta nueva forma de interactuar con el arte está abriendo nuevas posibilidades para los artistas y coleccionistas por igual. [29]

Además, la tokenización está comenzando a encontrar aplicaciones en otras áreas, como los coleccionables deportivos. Plataformas como Sorare y NBA Top Shot han aprovechado la tecnología Blockchain para crear tokens de coleccionables deportivos que están revolucionando la forma en que los aficionados interactúan con sus deportes favoritos. En lugar de coleccionar tarjetas físicas, los usuarios pueden ahora poseer y comerciar representaciones digitales únicas de sus jugadores y momentos deportivos favoritos.

### **3.2 EL MERCADO INMOBILIARIO ACTUAL**

La inversión inmobiliaria es una de las más antiguas y potentes formas de inversión que hay. Por definición, el inversor inmobiliario es aquel individuo o empresa que invierte activamente en bienes raíces [30] entendiéndose los bienes raíces como un bien inmueble, aquel anclado a la tierra y que no se puede mover. Estos inversores pueden ser bancos, bancos de inversión inmobiliaria (REIB), business angels, capitalistas de riesgo, inversores personales, inversores inmobiliarios o fondos de cobertura. Se entiende por inversión

inmobiliaria el financiamiento, asesoría, compra, desarrollo, alquiler y venta de inmuebles con la intención de obtener una rentabilidad de ellos. Se puede dividir el mercado en cuatro grupos dependiendo del tipo de inversión del que se trate [30]:

- Propiedades residenciales: se trata de inmuebles destinados a que vivan las personas.
- Propiedades comerciales: tiendas minoristas, mayoristas, oficinas, instalaciones de almacenamiento, almacenes generales, hoteles. Más costosa y complicada que la anterior con contratos más largos.
- Propiedades industriales: cualquier tipo de bienes raíces que generan rendimientos a los clientes por su uso como por ejemplo almacenes industriales y fábricas.
- Propiedades de uso mixto: propiedades que combinan varias categorías.

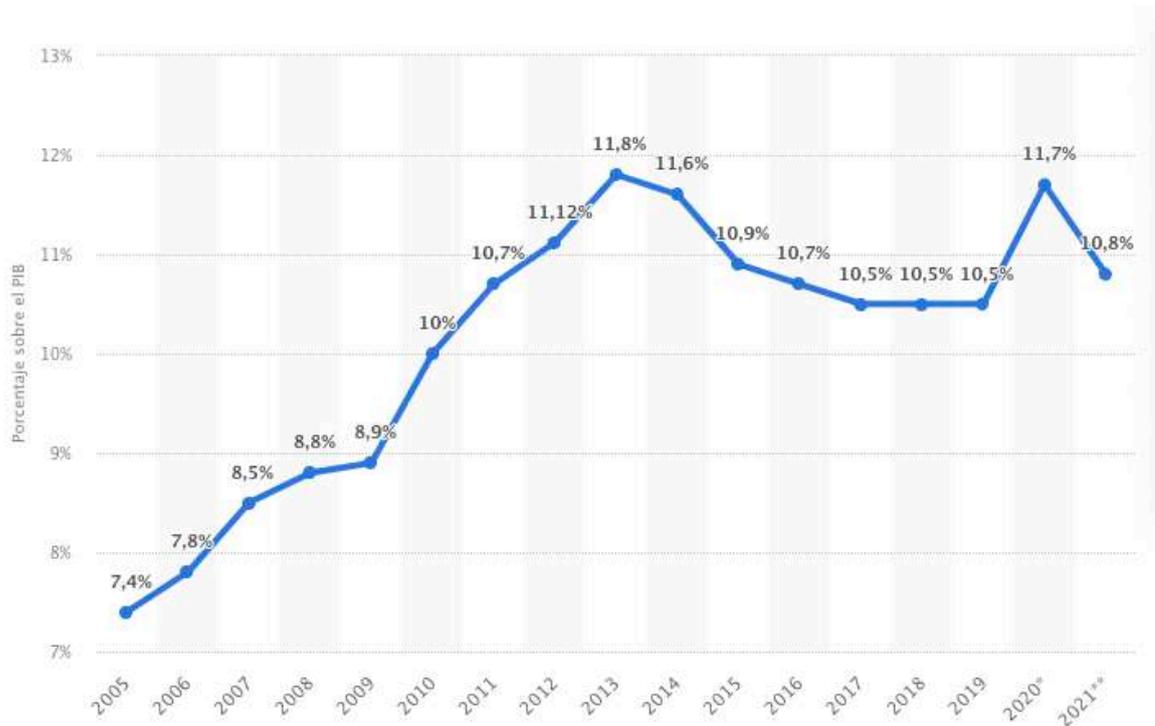
En cuanto a las estrategias y formas de inversión en inmuebles existen innumerables técnicas, cada día más variadas y creativas, aunque la más comunes son el alquiler tras compra y la venta idealmente por un precio mayor.

El mercado de compraventa de inmuebles en España, como se puede observar en la Figura 7, sufrió una fuerte caída con la pandemia de COVID-19, sin embargo, en el año 2021, recuperó e incluso superó los niveles previos a la pandemia con alrededor de 50.000 inmuebles involucrados en este tipo de operaciones [31].



Figura 7 - Compraventa de viviendas en España (Fuente: Cortesía de KPMG) [31]

Para poner más en contexto y ubicar las dimensiones y peso del mercado inmobiliario, el gráfico de la Ilustración 1 muestra como han influido desde el 2005 las actividades inmobiliarias en España resultando en un 10,5% o más en los últimos 5 años del total del PIB español, calculado en 1,328 billones de euros en 2022 [32]. Este sector es pues de una gran relevancia en el contexto nacional y un gran reclamo para el inversor internacional.



*Ilustración 1 - Peso de las actividades inmobiliarias sobre el PIB de España (Fuente: Statista)*

Actualmente, el mercado inmobiliario lleva consigo tediosos, lentos y costosos procesos burocráticos que involucran intermediarios como abogados, notarios y agentes inmobiliarios haciendo el proceso de adquisición de un inmueble ineficiente en la mayoría de las ocasiones.

Según un estudio sobre la experiencia de compra y venta del portal Fotocasa en el año 2021, [33] el 24% de los compradores de ese año tardaron entre 2 y 4 meses en cerrar todo el proceso, el 19% entre 4 y 6 meses, el 15% entre 6 y 12 meses y el 9% más de dos años. Estos largos tiempos nuevamente reafirman la ineficiencia del proceso.

Además de la demora, hay que tener en cuenta los grandes costes asociados. En España, la compraventa de inmuebles hay que escriturarla ante notario, este cobrará entre el 0,2% y el 0,5% sobre el valor del inmueble, además, el interesado se hará cargo del coste de la copia de la propia escritura, lo que ronda los 15 euros. Asimismo, un registrador de la propiedad ha de inscribir al interesado en el Registro de la Propiedad, lo que supone entre un 0,1% y

un 0.25% sobre el precio del inmueble. Además de los gastos administrativos comentados, en muchas ocasiones las agencias inmobiliarias actúan de intermediarios en los procesos de compraventa y alquiler. En cuanto a sus honorarios existe un gran abanico de posibilidades, mientras que las inmobiliarias tradicionales cobran entre un 3% y un 7% del precio de la vivienda según el portal Idealista [34], las inmobiliarias online suelen tener una horquilla fija de entre 1.000 y 5.000 euros.

### **3.2.1 PROCESO DE COMPRAVENTA ACTUAL**

Según datos del Ministerio de Justicia de España [35], el Colegio de Registradores de España [36] y de la Agencia Tributaria de España [37], el proceso de compraventa de un inmueble en España sigue los siguientes pasos:

- Selección del inmueble por parte del comprador y negociación del precio por ambas partes, habitualmente, requiere una visita física al inmueble por parte de la parte interesada.
- Firma del contrato de Arras: Se trata de un contrato privado entre las dos partes mediante el cual se pacta la venta del inmueble, se entrega una cantidad de dinero como señal y este queda reservado. Este contrato puede ser penitencial, es decir, en caso de incumplimiento, el incumplidor pierde la cantidad entregada, o confirmatorio, es decir, se podría exigir el cumplimiento o una resolución con indemnización por daños y perjuicios.
- Preparación de la escritura pública de compraventa: Documento por el cual se certifica la transacción y es firmado ante notario. Dicho documento es firmado ante notario e incluye la descripción de la propiedad, su precio de venta y cualquier otra condición.
- Pago de Impuestos: En España, este tipo de transacciones inmobiliarias está sujeta a dos tipos de impuestos: IVA para viviendas de obra nueva y el ITP o Impuesto de transmisiones Patrimoniales para viviendas de segunda mano. El vendedor ha de pagar la Plusvalía Municipal si el valor del terreno ha aumentado en el periodo de tiempo en el que este lo ha poseído.

- Inscripción en el Registro de la Propiedad: La escritura se lleva para su inscripción al Registro de la Propiedad garantizando la legalidad de la posesión por parte del nuevo propietario.

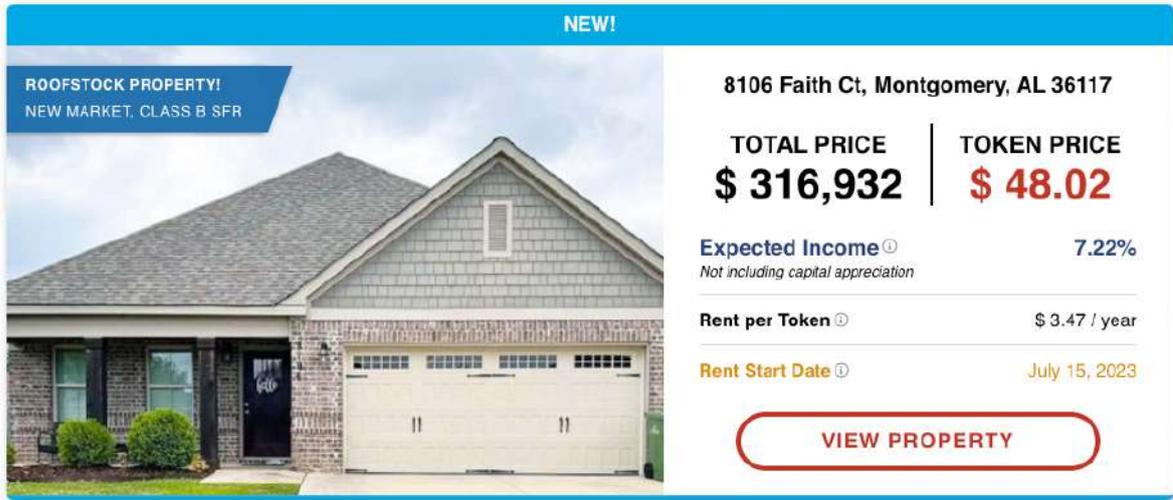
### **3.3 PROYECTOS BLOCKCHAIN INMOBILIARIOS**

Habiendo visto las dimensiones del mercado inmobiliario y las grandes oportunidades que lleva consigo, resulta lógico pensar que se desarrollen soluciones para paliar en la medida de lo posible las barreras de entrada para el usuario común y se flexibilicen los procesos.

En la ciudad de South Burlington, Vermont, Estados Unidos, en el año 2019, la compañía de Blockchain Propy [38] llevó a cabo una prueba para implementar una nueva forma de registrar las transacciones inmobiliarias, esta plataforma según estaba planteada enviaba la documentación a las oficinas públicas como cualquier otra transacción inmobiliaria, sin embargo, incluía la ubicación de la misma en la Blockchain de Propy donde posteriormente, la administración verificaba que la había recibido y la introducía en su sistema de registro. Sin embargo, el proyecto piloto no triunfó. [39]

Precisamente esta empresa, Propy, es una de las más avanzadas en el sector Blockchain inmobiliario ya que cuenta con una plataforma que ofrece un amplio listado de propiedades a la venta para sus clientes.

Otra plataforma interesante en el mundo de la tokenización inmobiliaria es RealT [39], la compañía americana promueve la inversión en tokens basados en rentas de inmuebles. La empresa pone a la venta partes alícuotas de un inmueble y ofrece información sobre su precio total, el precio del token y la rentabilidad esperada de dicho token basado en un contrato de alquiler que gestiona la propia compañía.



**NEW!**

**ROOFSTOCK PROPERTY!**  
NEW MARKET, CLASS B SFR

**8106 Faith Ct, Montgomery, AL 36117**

<b>TOTAL PRICE</b>	<b>TOKEN PRICE</b>
<b>\$ 316,932</b>	<b>\$ 48.02</b>

**Expected Income** 7.22%  
Not including capital appreciation

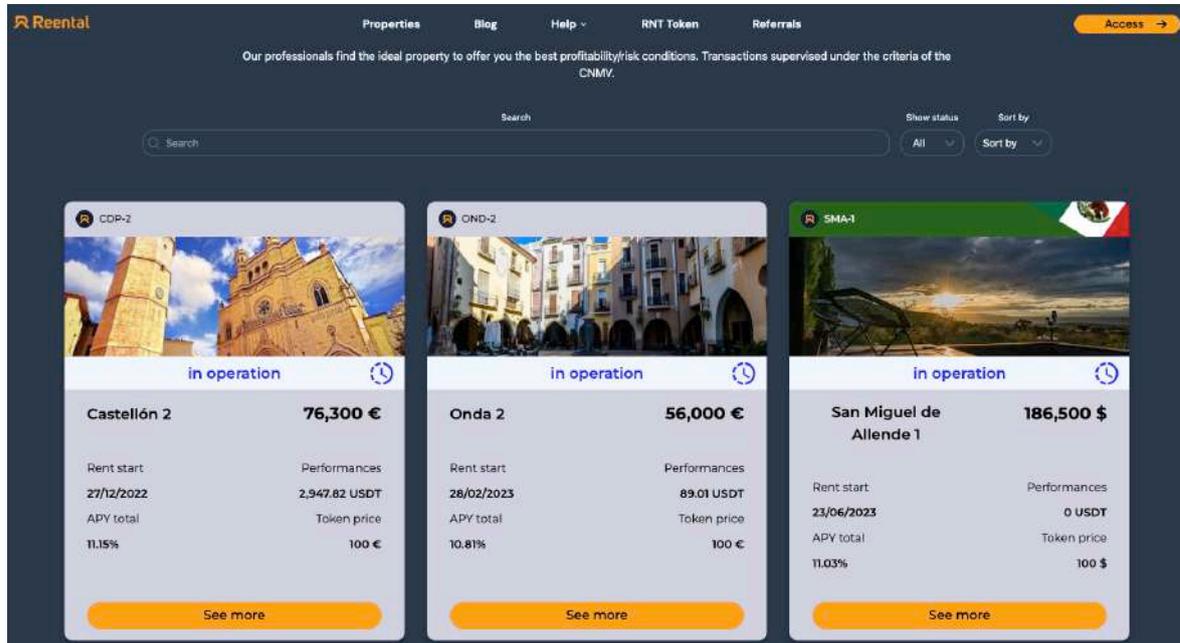
**Rent per Token** \$ 3.47 / year

**Rent Start Date** July 15, 2023

**VIEW PROPERTY**

*Ilustración 2 - Ejemplo de anuncio de la compañía RealT [40]*

En España, Reental [41] es el referente en el sector. La empresa ha sufrido un gran crecimiento en el último año multiplicando por nueve su oferta de inmuebles en los últimos 15 meses. Según cuenta su CEO y cofundador, Eric Sánchez, la idea surgió a raíz de la falta de capital para realizar una inversión inmobiliaria que propició que varios amigos juntaran su dinero y procedieran a adquirir el inmueble entre todos. La forma que encontraron de escalar ese concepto con poca burocracia y de manera simple para el usuario final fue a través de la tokenización de inmuebles. Actualmente cuentan con 37 inmuebles con tokens a la venta, mayoritariamente en España, aunque también cuentan con propiedades en Miami y México.



*Ilustración 3 - Pantalla "Properties" de Reental.co*

El modelo de Reental es muy similar al comentado con anterioridad en RealT. El equipo de la empresa busca oportunidades de inmuebles atractivos tanto para su alquiler, como para la renta de habitaciones o vacacional en diferentes ubicaciones atractivas para un posible arrendador, los reforma y equipa y procede a su posterior alquiler ofreciendo a sus clientes la posibilidad de participar de este a través de cada token. Este token ofrece información de su rentabilidad anualizada y es custodiado por el cliente en su propia cartera. Reental se encuentra actualmente en el proceso de lanzamiento de su propio token, el cual permitirá a sus poseedores acceder a ciertos beneficios e incluso a la posibilidad de financiación, a parte de la propia especulación de toda criptomoneda. En una entrevista reciente<sup>3</sup>, Eric Sánchez comenta como un piso de 150.000 ubicado en España euros agotó todos sus tokens en 2 minutos y otro ubicado en Miami de 700.000\$ se agotó en 5 horas.

<sup>3</sup> [1] “Eric Sánchez, CEO de reental,” YouTube, <https://www.youtube.com/watch?v=tSgOirXX3Ug&amp;t=47s> (accessed Jul. 4, 2023).

Por todo ello es lógico pensar que existe y tiene sentido en el contexto actual una aplicación de las características de la desarrollada.

## **Capítulo 4. DEFINICIÓN DEL TRABAJO**

### **4.1 JUSTIFICACIÓN**

No es ninguna sorpresa que el mercado inmobiliario es uno de los más fuertes e importantes de cualquier economía [42] ya que la vivienda es un bien de máxima necesidad para cualquier individuo. Como se ha comentado en apartados anteriores, el mercado de bienes raíces tradicional presenta ciertos problemas a la hora de ser ágil y sencillo para el usuario medio, acostumbrado a la inmediatez y eficiencia de los procesos de compra de nuestros días.

Este proyecto surge como respuesta a la necesidad de paliar las limitaciones y aprovechar las oportunidades que la tecnología, en concreto la tecnología Blockchain [7] nos ofrece como se ha podido ver en muchos sectores de la industria. Se busca explorar las posibles soluciones que agilicen los procesos de compraventa y gestión de las propiedades mediante una red de transacciones segura, transparente y fiable.

Las soluciones Blockchain pueden transformar de una manera radical la manera en la que son realizadas las transacciones de propiedad, eliminando intermediarios, aumentando la eficiencia y velocidad de los procesos, pero sin comprometer la seguridad e integridad de ninguna de las dos partes y los trabajos previos lo han demostrado. Precisamente este concepto de integridad y seguridad ha sido muy relevante en el planteamiento de este proyecto ya que, el mercado inmobiliario es uno de los más propensos a la corrupción. Según el informe “La corrupción en España: rasgos y causas esenciales” de 2015 por M.Villoria [43] más de 600 municipios españoles tienen algún escándalo de corrupción en el sector, por ejemplo, el 60% de los municipios de Murcia y el 40% de los de Canarias cuentan con algún caso de corrupción inmobiliaria.

El mercado inmobiliario debe de democratizarse y abrirse al público al igual que lo han hecho muchos otros mercados financieros

## **4.2 OBJETIVOS**

En este apartado se expondrán los objetivos tenidos en cuenta en el diseño y la elaboración del Trabajo Fin de Grado para crear una solución descentralizada para la gestión y comercialización de inmuebles:

- Desarrollar un contrato inteligente que cree los NFTs en Ethereum con distintas características e información sobre el inmueble y otro para elaborar su proceso de compraventa.
- Crear un método de compraventa en el que intervengan más de dos agentes para garantizar la seguridad e integridad de las transacciones y su supervisión.
- Implementar todas las funciones deseadas en una interfaz de usuario intuitiva y simple. Ya que el fin último de este Trabajo Fin de Grado es el de democratizar el proceso de compraventa de inmuebles, es importante que la aplicación sea agradable visualmente y que este pensada para que pueda ser usada por cualquier usuario sin importar su experiencia en Blockchain ni su nivel de conocimiento.
- Estructurar todo el mecanismo descrito en una red Blockchain local de prueba que permita comprobar el correcto funcionamiento de todas las funciones descritas para poder llevarla a cabo en un entorno real en un futuro.

## **4.3 METODOLOGÍA**

Puesto que para la entrega de este proyecto existía una fecha límite, ya que el proyecto se ha realizado a lo largo de un curso académico, se ha empleado una metodología en cascada para organizar su progreso y consecución de objetivos. Se ha elegido este modelo de organización del proceso debido a su estructura lineal, permitiendo un seguimiento preciso del proceso de desarrollo, así como la detección de posibles retrasos. [44]

Este tipo de metodología se caracteriza por dividir un proyecto grande en subetapas más pequeñas que se deben completar en orden.

	Oct	Nov	Dic	En	Feb	Mar	Abr	May	Jun
Análisis									
Diseño									
Desarrollo									
Prueba									
Documentación									

*Tabla 2 - Diagrama de Gant del proyecto*

Como se puede observar, en los meses de octubre, noviembre y diciembre se produjo un análisis del proyecto, investigando las opciones existentes y considerando las diferentes formas de aplicación de los requisitos planteados con las tecnologías disponibles, así como teniendo una aproximación minuciosa al mundo del Blockchain y los activos digitales.

En diciembre se empezó, una vez finalizado el análisis con el diseño del proyecto, valorando las distintas opciones de arquitecturas y software que más se adecúan a la viabilidad del proyecto, así como al nivel de conocimiento del desarrollador.

A mediados de enero se procedió al desarrollo de la aplicación descentralizada atendiendo al lanzamiento de la Blockchain local utilizando HardHat para poder probar los contratos y funciones. Tras muchos avances y retrocesos, entre finales de mayo y principios de junio finalizó el desarrollo y se probó el sistema.

A lo largo de todo el proceso se ha producido el registro de las diferentes características y escenarios en la documentación del proyecto, poniendo énfasis en junio como mes en el que se han completado los últimos apartados relativos a la parte práctica y los resultados del mismo.

## **4.4 PLANIFICACIÓN Y ESTIMACIÓN ECONÓMICA**

Los recursos materiales empleados en este Trabajo Fin de Grado son un ordenador portátil y un monitor que a continuación voy a describir:

### **4.4.1 COSTES MATERIALES**

#### *Ordenador Portátil MacBook Pro 2021*

PROCESADOR	APPLE M1 PRO CHIP
NÚMERO DE NÚCLEOS	8
NÚCLEOS GPU	8
SISTEMA OPERATIVO	MACOS VENTURA 13.4
PANTALLA	14 PULGADAS
MEMORIA RAM	16 GB
ALMACENAMIENTO	1 TB
PRECIO	2249 €

*Tabla 3 - Características técnicas ordenador portátil*

*Monitor HP M22f*

TAMAÑO DE LA PANTALLA	22 PULGADAS
RESOLUCIÓN	FULL HD 1920X1080, 75HZ
TIPO DE PANEL	IPS LED
AUDIO	ALTAVOCES INCORPORADOS
PRECIO	129€

*Tabla 4 - Especificaciones Monitor*

Ambos dispositivos tienen una vida fiscal útil de 4 años o 35.040 horas según la Agencia Tributaria [37]. Ambos dispositivos han sido utilizados para otros fines a la vez que se desarrollaba el proyecto, por lo que se va a distribuir el coste en función del tiempo de uso aproximado que es de 900 horas (se puede ver una aproximación más detallada en la Tabla 5). Teniendo en cuenta estas horas se lleva a cabo la amortización de los materiales empleados.

<i>Actividad</i>	<i>Horas</i>
Organización, reuniones y planificación	15
Análisis y estudio	155
Diseño	175
Desarrollo	225
Pruebas	30

Documentación	300
<b>TOTAL</b>	<b>900</b>

*Tabla 5 - Distribución de las horas*

$$\text{Coste por hora del portátil} = \frac{2249\text{€}}{35040 \text{ horas}} \approx 0.0642\text{€/hora}$$

$$\text{Coste proyecto portátil} = \frac{0.0642\text{€}}{\text{hora}} \times 900 \text{ horas} \approx 57'76\text{€}$$

*Ecuación 1 - Cálculo del coste del portátil al proyecto*

$$\text{Coste por hora del monitor} = \frac{129\text{€}}{35040 \text{ horas}} \approx 0.0037\text{€/hora}$$

$$\text{Coste proyecto monitor} = \frac{0.0037\text{€}}{\text{hora}} \times 900 \text{ horas} \approx 3'31\text{€}$$

*Ecuación 2 - Cálculo del coste del monitor al proyecto*

Esto en lo relativo al hardware, en lo que concierne al software, todos los programas empleados en el desarrollo del Trabajo Fin de Grado son gratuitos excepto macOS que es un software de pago incluido en el precio del ordenador portátil y cuyo coste ya está contemplado.

#### **4.4.2 COSTES DE DESARROLLO**

El coste total de gas de una transacción es de 4.573.412 gwei o 8'03 € al precio en el momento de la escritura de este documento. Además, hay que tener en cuenta el coste del servicio Pinata para gestionar los archivos IPFS que se van a subir a la red. Para ello tomamos como referencia su plan de pago más adecuado a los fines de este proyecto, el denominado Fiesta [45], el cual tiene un coste de 100\$ mensuales, lo que al momento de la redacción de este documento supone 91'6€ mensuales.

<i>Coste</i>	<i>Precio</i>
Ordenador portátil	57'76€
Monitor	3'31€
Desplegar contratos	8.03€
Pinata	91'6€/mes

*Tabla 6 - Resumen de los costes de desarrollo*

#### **4.4.3 RECURSOS HUMANOS**

Para el desarrollo de este Trabajo Fin de grado, se ha requerido de un desarrollador de *software*. Según los datos de la plataforma de reclutamiento y valoración de empleos Talent, el salario medio de un desarrollador de software en España es de 14,62 € / hora [46].

$$\text{Sueldo hora desarrollador} = 900 \text{ horas} \times 14,62\text{€ por hora} = 13.158\text{€}$$

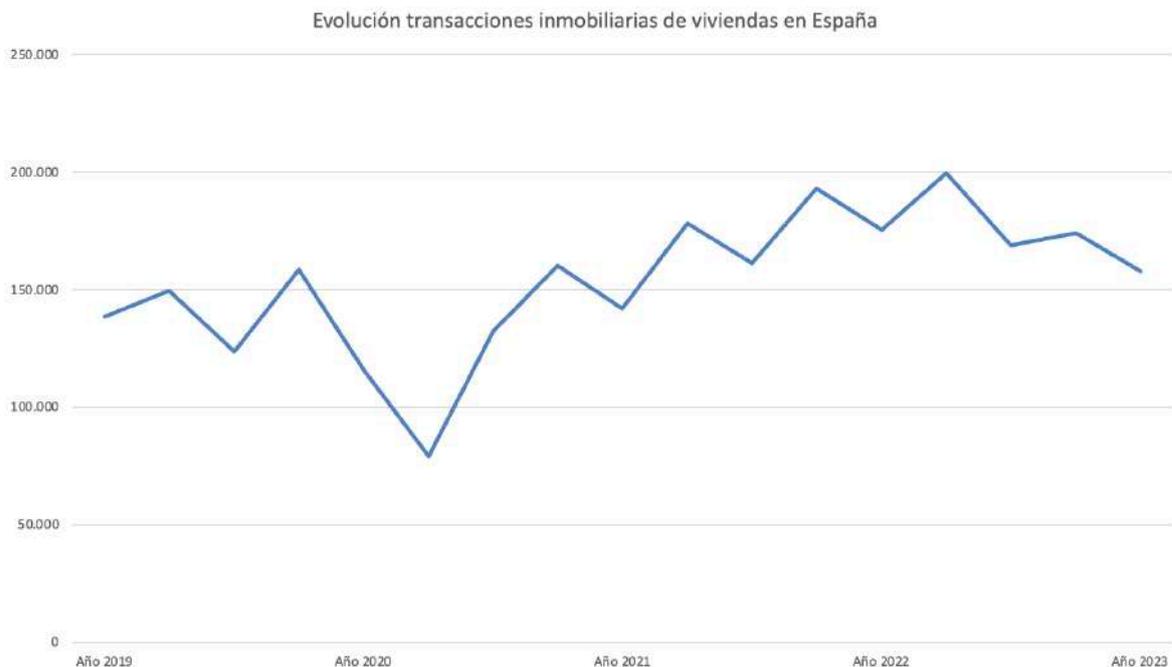
Aparte del sueldo del desarrollador principal, también es necesario contratar a un desarrollador que mantenga la aplicación, por lo que al menos un programador de software deberá estar contratado al año, lo que hace un total de 28.500 € al año según datos de Talent nuevamente.

#### **4.4.4 PRESUPUESTO TOTAL**

Teniendo en cuenta los datos presupuestarios de desarrollo y mantenimiento contemplados en los apartados anteriores, procedemos al análisis de los beneficios probables.

Se contemplarán dos posibles escenarios, uno más optimista y otro más pesimista.

Según datos del Ministerio de Transportes, Movilidad y Agenda Urbana del Gobierno de España, en el año 2022 se produjeron un total nacional de 717.734 transacciones inmobiliarias de viviendas en términos de compraventa [47]. Cabe destacar que se utilizarán datos de España ya que son los más fiables y actualizados de los que se dispone de un país que sirva de referencia en este proyecto, sin embargo y al tratarse de una aplicación web, los clientes potenciales de este proyecto son cualquier individuo del mundo con conexión a internet.



*Figura 8 - Evolución del número de transacciones inmobiliarias de viviendas en España por trimestre  
(Fuente: Elaboración propia, con datos del Ministerio) [47]*

Como se puede ver en la Figura 8 y exceptuando los efectos de la pandemia en 2020, el número de transacciones se mantiene por encima de las 150.000 aproximadamente cada trimestre en los últimos dos años. Sin embargo, el número de transacciones varía de año a año y se ve muy influenciado por las variables macroeconómicas del entorno.

Teniendo en cuenta la cuota de gas de cada transacción, de media se ha estimado que cada proceso de compraventa requiere de unos 150.000 gwei, lo que supone unos 0'27 € en el momento de escritura de este documento, por lo que es muy poco margen para recuperar

beneficios, por ello se ha decidido cobrar al usuario una comisión fija de 10 € por transacción.

#### ***4.4.4.1 Escenario optimista***

Un escenario optimista para una *start-up* que se introdujera de manera exitosa en el mercado inmobiliario español sería aquella que contase con una cuota de mercado de entre un 1% y un 3% de las transacciones totales. Teniendo en cuenta la novedad del sistema planteado y la robustez y establecimiento del mercado inmobiliario actual, muy consolidado, vamos a suponer un 1% de cuota de mercado.

Por tanto, el cálculo de los ingresos sería el siguiente:

$$1\% \times 717.734 \text{ operaciones} \times 10\text{€} = 71.773'4 \text{ €}$$

	<i>Precio anual</i>
Gastos de mantenimiento	29.700€
Ingresos estimados	71.773'4 €
<b>BENEFICIO</b>	<b>42.073'4€</b>

*Figura 9 - Cálculo de los beneficios brutos anuales*

Hay que resaltar que el coste de mantenimiento es un coste único para la aplicación independientemente de la cantidad de países en los que se opere, mientras que la estimación de ingresos se ha hecho únicamente en España como se ha comentado con anterioridad.

Teniendo en cuenta el coste inicial de 13.158 €, el primer año se ingresarían 28.915'4 € procedentes únicamente del mercado español, por lo que hace ser optimistas teniendo en cuenta que se generarían beneficios solo en un país.

#### 4.4.4.2 *Escenario pesimista*

Un escenario pesimista para una *start-up* en su primer año sería una cuota de mercado de entre un 0'1% y un 0'5%, por lo que se asumirá el caso menos favorable.

$$0'1\% \times 717.734 \text{ operaciones} \times 10\text{€} = 7.177'34 \text{ €}$$

	<i>Precio anual</i>
Gastos de mantenimiento	29.700€
Ingresos estimados	7.177'34 €
<b>BENEFICIO</b>	<b>-22.522'66 €</b>

*Figura 10 - Ingresos brutos estimados caso menos favorable*

Como se puede ver, se producirían pérdidas, en especial el primer año al que habría que añadirle el coste inicial, por lo que se perderían 35.680'66 €.

A vistas de estos resultados, hace ser optimista teniendo en cuenta el carácter global de la aplicación.

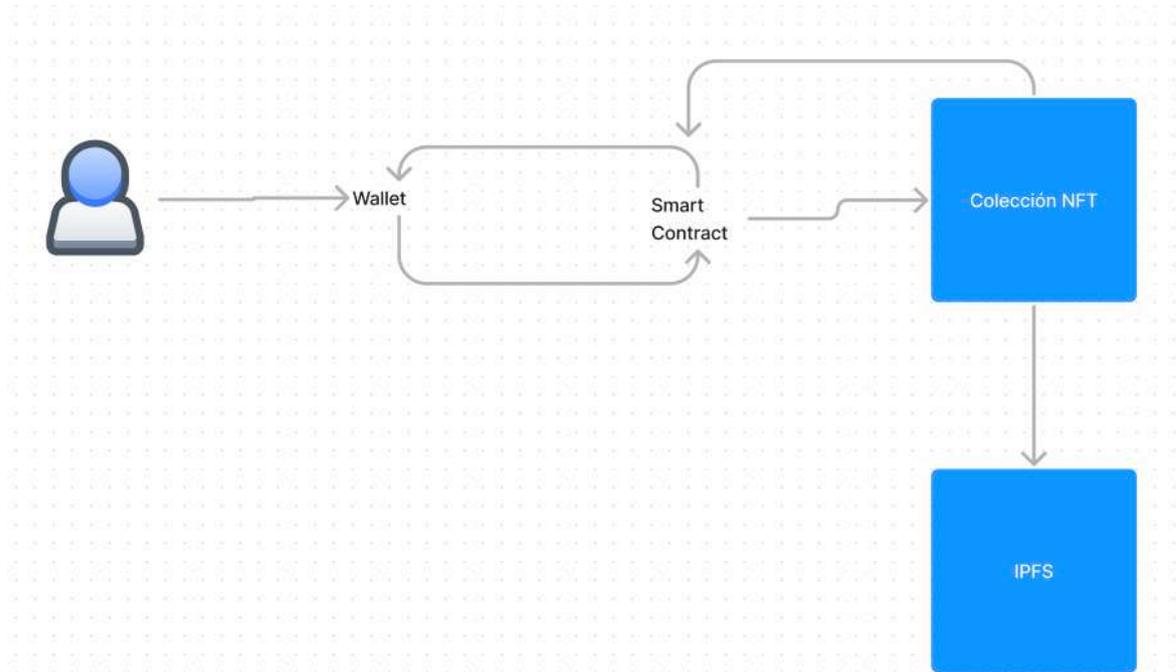
## Capítulo 5. SISTEMA/MODELO DESARROLLADO

En este capítulo se expondrá en detalle el sistema elaborado en este Trabajo de Fin de Grado, una aplicación descentralizada que revoluciona la gestión y transacción de propiedades inmobiliarias. Nuestro sistema, basado en tecnología blockchain, consta de dos contratos inteligentes: uno para la creación de tokens no fungibles (NFTs) que representan propiedades individuales, y otro para facilitar la compraventa segura de estos NFTs. El uso de la blockchain y los contratos inteligentes permite una transparencia óptima y una inmutabilidad que garantiza la seguridad en cada transacción. Además, se ha diseñado una interfaz web sencilla e intuitiva para que cualquier usuario pueda interactuar con la plataforma sin complicaciones. Este sistema busca hacer accesible el mercado inmobiliario para todos, eliminando las barreras habituales y democratizando el proceso de compraventa de inmuebles.

### 5.1 DISEÑO DEL SISTEMA

En el presente proyecto, se ha desarrollado un *front-end* y un *back-end*, para el *front-end* se ha utilizado React ya que permite la fácil integración del entorno gráfico así como la compatibilidad y soporte con la cartera MetaMask.

En la parte del *back-end*, se ha empleado Ethereum, IPFS, HardHat y Node.js. Los contratos inteligentes se encargan de generar inmuebles y almacenarlos en IPFS, sistema que permite guardar la información y hacerla accesible en todo momento de manera descentralizada y segura.



*Figura 11 - Flujo del diseño (Elaboración propia)*

En la Figura 11 se detalla el flujo del diseño del sistema. En este proyecto, los usuarios se conectan a la aplicación a través de su cartera de MetaMask. Una vez conectados a la aplicación, la forma de interactuar es a través de los contratos inteligentes que se comunican con la colección NFT de inmuebles ya sea para comprar o para vender bienes raíces. Esta colección se guarda y gestiona a través de IPFS.

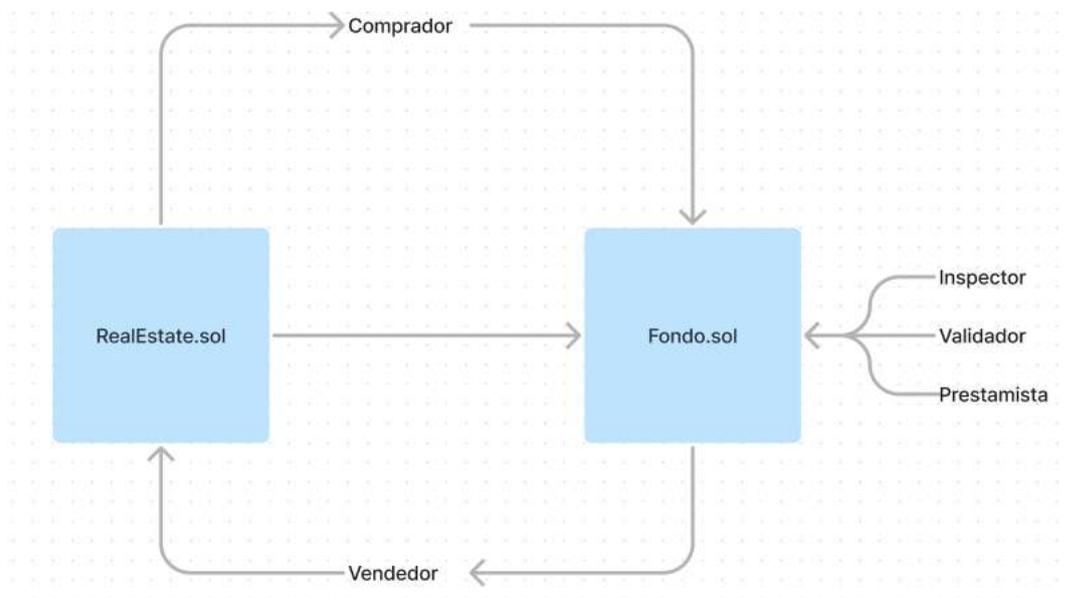


Figura 12 - Diseño de la lógica del sistema (elaboración propia)

Como se ha comentado con anterioridad, uno de los principales requisitos de esta aplicación era la integridad y seguridad de las transacciones inmobiliarias, para ello se ha ideado un sistema de compraventa supervisado y en el que los fondos se encuentran protegidos en todo momento. Este sistema definido en la Figura 12 muestra el proceso de fondo de garantía que sigue la aplicación. En primer lugar, el contrato RealEstate.sol crea los NFT y les atribuye sus características principales. Una vez creado, el contrato Fondo.sol hace las veces de fondo de garantía. Analizando el proceso de compra de un inmueble podemos ver la actuación de cada uno de los agentes que intervienen en este contrato: cuando una cartera manda la orden de comprar un NFT, en primer lugar se bloquean sus fondos a través del contrato, seguidamente, una cartera diferente, la cual hace de validador de la operación la aprueba; a continuación, un inspector de la operación en su conjunto da el visto bueno y cuando esto ocurre, el prestamista confirma su operación y los fondos son liberados y entregados al vendedor quedando así registrada la operación dentro de la red Blockchain.

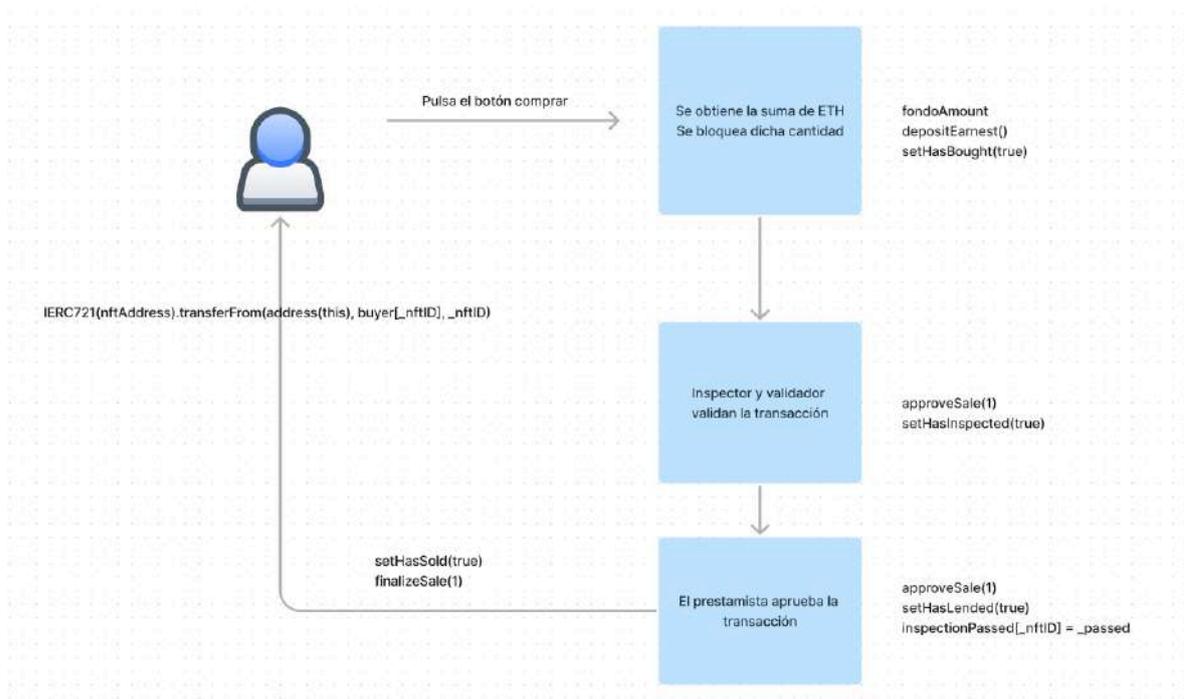
De esta forma y con la simple supervisión y confirmación de 3 cuentas distintas queda sellada una operación en el sistema planteado, creando así una rutina de compraventa con garantías.

## 5.1.1 CASOS DE USO

A continuación, se va a exponer las diferentes situaciones de uso:

### 5.1.1.1 Compra aceptada

En la Figura 13 se observa a alto nivel las funciones que intervienen en el proceso de compra de un inmueble hasta llegar a la función de IERC721 transferFrom() la cual es la que finalmente actualiza la propiedad del NFT.



*Figura 13 - Proceso de compra*

### 5.1.1.2 Compra cancelada

En cualquier parte del proceso descrito con anterioridad, una negativa por parte del prestamista, inspector o validador podría causar la invocación de la función cancelSale(), la cual devolvería los fondos retenidos al comprador y cancelaría la transacción.

## 5.2 IMPLEMENTACIÓN

Una vez estructurado a nivel conceptual el sistema desarrollado, se analizarán los componentes que estructuran dicho sistema.

### 5.2.1 REALSTATE.SOL

```
//SPDX-License-Identifier: Unlicense
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/utils/Counters.sol";
import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
import "@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol";

contract RealEstate is ERC721URIStorage {
    using Counters for Counters.Counter;
    Counters.Counter private _tokenIds;

    constructor() ERC721("Real Estate", "REAL") {}

    function mint(string memory tokenURI) public returns (uint256) {
        _tokenIds.increment();

        uint256 newItemId = _tokenIds.current();
        _mint(msg.sender, newItemId);
        _setTokenURI(newItemId, tokenURI);

        return newItemId;
    }

    function totalSupply() public view returns (uint256) {
        return _tokenIds.current();
    }
}
```

*Figura 14 - Código fuente del contrato RealEstate.sol*

Como se puede ver en el bloque de código de la Figura 14, este contrato escrito en Solidity, el contrato implementa las funcionalidades de un token no fungible (NFT) a través del estándar ERC721. Se han usado varias bibliotecas de OpenZeppelin, una librería segura y comunitariamente auditada de contratos inteligentes.

El contrato se detalla a continuación:

- `import "@openzeppelin/contracts/utils/Counters.sol"`: Importa la librería Counters de OpenZeppelin, que proporciona un contador seguro para incrementar o decrementar su valor.
- `import "@openzeppelin/contracts/token/ERC721/ERC721.sol"`: Importa el contrato base ERC721 de OpenZeppelin que implementa la interfaz estándar ERC721 para tokens no fungibles.
- `import`  
`"@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol"`: Importa el contrato ERC721URIStorage que extiende el ERC721 con una funcionalidad de almacenamiento URI para tokens.
- En la línea 6 se define el contrato RealEstate que hereda de ERC721URIStorage que es la que se encarga de gestionar el URI (metadatos) de los tokens NFT.
- `using Counters for Counters.Counter`: Habilita el uso de funciones de la librería Counters.
- `Counters.Counter private _tokenIds`: Declara una variable privada `_tokenIds` de tipo Counter para llevar un registro de los tokens creados<sup>4</sup>.
- `constructor() ERC721("Real Estate", "REAL") {}`: Define el constructor del contrato que llama al constructor del contrato ERC721 con los argumentos "Real Estate" y "REAL" que representan el nombre y el símbolo del token no fungible, respectivamente.
- `function mint(string memory tokenURI) public returns (uint256) {` : Define una función pública `mint` que permite la creación de nuevos tokens. Acepta una cadena de caracteres `tokenURI` que representa los metadatos del token, devolviendo el ID del nuevo token.
- `_tokenIds.increment()`: Incrementa el contador de tokens creados.
- `uint256 newItemId = _tokenIds.current()`: Crea un nuevo ID para el token a partir del contador de tokens.

---

<sup>4</sup> La creación de un NFT se conoce como `mintear` un NFT.

- `_mint(msg.sender, newItemId)`: Crea un nuevo token ERC721 con el ID `newItemId` y lo asigna al remitente de la transacción.
- `_setTokenURI(newItemId, tokenURI)`: Asigna el URI de metadatos al token creado.
- `function totalSupply() public view returns (uint256) {` : Define una función pública de vista `totalSupply` que devuelve el número total de tokens minteados hasta el momento.

A modo de resumen y como forma de conceptualmente visualizar el contrato, este se encarga de crear a través de la función `mint` un nuevo NFT único con un registro seguro gracias al contador de `OpenZeppelin` y a `ERC721` que asigna un URI (metadatos) único. Además, se ha creado una función denominada `totalSupply()` que lleva el registro del total de NFTs.

## 5.2.2 FONDO.SOL

```
interface IERC721 {
    function transferFrom(
        address _from,
        address _to,
        uint256 _id
    ) external;
}

contract Fondo {
    address public nftAddress;
    address payable public seller;
    address public inspector;
    address public lender;

    modifier onlyInspector() {
        require(msg.sender == inspector, "Solo inspector");
        _;
    }

    modifier onlyBuyer(uint256 _nftID) {
        require(msg.sender == buyer[_nftID], "Solo comprador");
        _;
    }

    modifier onlySeller() {
        require(msg.sender == seller, "Solo vendedor");
        _;
    }

    mapping(uint256 => bool) public isListed;
    mapping(uint256 => uint256) public escrowAmount;
}
```



```
mapping(uint256 => address) public buyer;
mapping(uint256 => bool) public inspectionPassed;
mapping(uint256 => uint256) public purchasePrice;
mapping(uint256 => mapping(address => bool)) public approval;

constructor(
    address _nftAddress,
    address payable _seller,
    address _inspector,
    address _lender
) {
    nftAddress = _nftAddress;
    seller = _seller;
    inspector = _inspector;
    lender = _lender;
}

function list(
    uint256 _nftID,
    address _buyer,
    uint256 _purchasePrice,
    uint256 _escrowAmount
) public payable onlySeller {
    IERC721(nftAddress).transferFrom(msg.sender, address(this), _nftID);
    isListed[_nftID] = true;
    purchasePrice[_nftID] = _purchasePrice;
    escrowAmount[_nftID] = _escrowAmount;
    buyer[_nftID] = _buyer;
}

function depositEarnest(uint256 _nftID) public payable onlyBuyer(_nftID) {
    require(msg.value >= escrowAmount[_nftID]);
}

function updateInspectionStatus(uint256 _nftID, bool _passed)
    public
    onlyInspector
{
    inspectionPassed[_nftID] = _passed;
}

function approveSale(uint256 _nftID) public {
    approval[_nftID][msg.sender] = true;
}

function finalizeSale(uint256 _nftID) public {
    require(inspectionPassed[_nftID]);
    require(approval[_nftID][buyer[_nftID]]);
}
```

```

require(approval[_nftID][seller]);
require(approval[_nftID][lender]);
require(address(this).balance >= purchasePrice[_nftID]);

isListed[_nftID] = false;

(bool success, ) = payable(seller).call{value: address(this).balance}(
    ""
);
require(success);

IERC721(nftAddress).transferFrom(address(this), buyer[_nftID], _nftID);
}

function cancelSale(uint256 _nftID) public {
    if (inspectionPassed[_nftID] == false) {
        payable(buyer[_nftID]).transfer(address(this).balance);
    } else {
        payable(seller).transfer(address(this).balance);
    }
}

receive() external payable {}

function getBalance() public view returns (uint256) {
    return address(this).balance;
}
}

```

*Figura 15 - Código contrato Fondo.sol*

Este contrato regula el proceso de listado de una propiedad por parte del comprador, el depósito de garantía por parte del comprador, la aprobación de la venta por todas las partes involucradas y la transferencia y pago del NFT.

Debido a su mayor extensión y complejidad se va a analizar a un más alto nivel que el contrato RealEstate.sol:

- En primer lugar, se define la interfaz que se va a utilizar, IERC721, la cual va a ser de gran ayuda a la hora de gestionar las direcciones y lógica del contrato.
- A continuación, se describen los modificadores de acceso y las variables a utilizar.

- **list**: Esta función permite a un vendedor listar una propiedad para la venta, estableciendo el precio de compra y la cantidad de depósito en garantía. El NFT correspondiente a la propiedad se transfiere al contrato.
- **depositEarnest**: Esta función permite al comprador depositar un importe en garantía en el contrato. Esta cantidad debe ser mayor o igual a la cantidad de depósito en garantía establecida por el vendedor.
- **updateInspectionStatus**: Esta función permite al inspector actualizar el estado de inspección de una propiedad. Si la propiedad pasa la inspección, la venta puede continuar.
- **approveSale**: Cualquier parte (comprador, vendedor o prestamista) puede aprobar la venta.
- **finalizeSale**: Una vez que todas las partes han aprobado y se han cumplido todas las condiciones (incluyendo la inspección y el precio correcto), la venta puede finalizarse. El contrato entonces transfiere el NFT al comprador y el pago al vendedor.
- **cancelSale**: Si la venta se cancela (por ejemplo, si la inspección falla), el contrato maneja la devolución del depósito en garantía.

### 5.2.3 IPFS

Como almacenar información en la Blockchain es una tarea muy costosa, se ha utilizado IPFS puesto que es un protocolo descentralizado, barato y es ampliamente utilizado en la comunidad Blockchain destacando a Uniswap [48] como una de las aplicaciones más importantes que hacen uso de este protocolo.

IPFS es un protocolo que no depende de un servidor centralizado único que pueda ser objeto de fallos y/o ataques por lo que proporciona una referencia inmutable a los datos almacenados haciendo que la información almacenada en un NFT no cambie.

En la elaboración de este proyecto, se han utilizado inmuebles de ejemplo, cada uno cuenta con una información asociada y una imagen del mismo. Esta imagen ha sido generada utilizando inteligencia artificial y posteriormente ha sido almacenada también en IPFS para mantener toda la información descentralizada.

```
{
  "name": "Madrid Retiro",
  "address": "Calle Ibiza, 31",
  "description": "Precioso ático dúplex a 3 minutos del Retiro",
  "image": "https://gateway.pinata.cloud/ipfs/QmeXUqW8axEARKwHr2hnTQeTQF17yMfQu7Nn8A13gXpGfj/Captura%20de%20pantalla%202023-06-28%20a%20las%2013.39.44.png",
  "id": "1",
  "atributes": [
    {
      "trait_type": "Precio de venta",
      "value": 35
    },
    {
      "trait_type": "Tipo de residencia",
      "value": "Apartamento"
    },
    {
      "trait_type": "Habitaciones",
      "value": 4
    },
    {
      "trait_type": "Baños",
      "value": 2
    },
    {
      "trait_type": "Metros cuadrados",
      "value": 320
    },
    {
      "trait_type": "Año de construcción",
      "value": 1965
    }
  ]
}
```

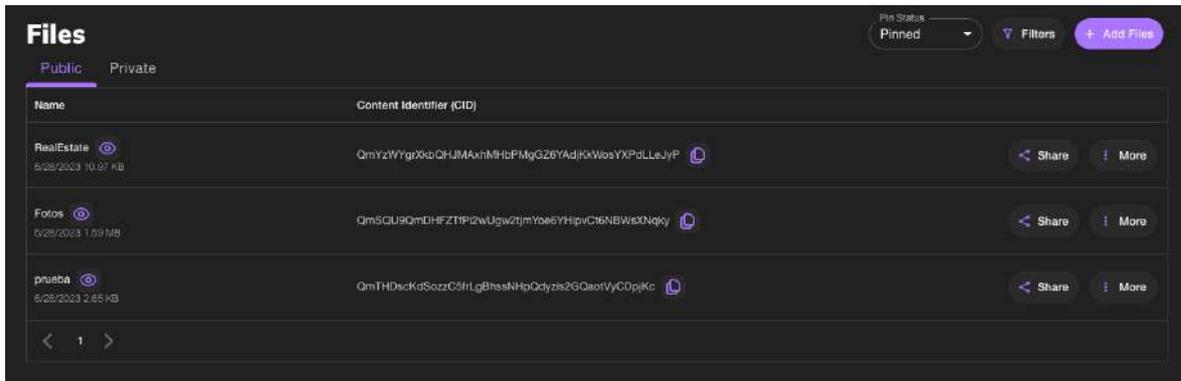
*Figura 16 - JSON con la información de cada inmueble*

Como se ilustra en la Figura 16, cada NFT tiene su archivo IPFS asociado que cuenta con sus características. Estas características son: Nombre, dirección, descripción, su imagen guardada a su vez en IPFS, su id, y unos atributos que lo describen como inmueble que son: precio de venta, tipo de residencia, habitaciones, baños, metros cuadrados y año de construcción.

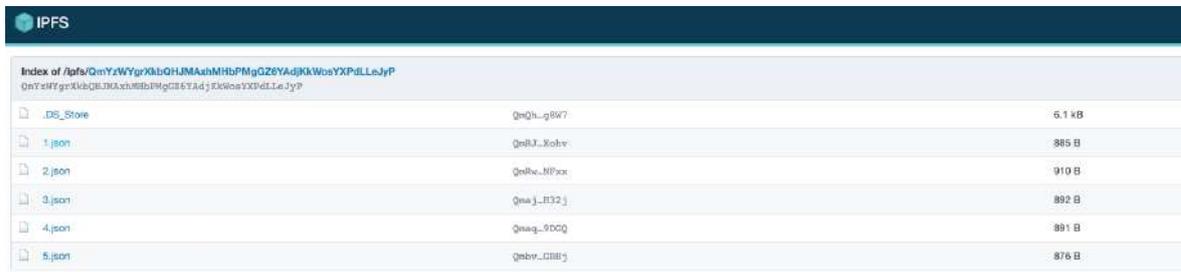
### **5.2.3.1 Pinata**

Para cargar archivos en la red IPFS se ha empleado Pinata. Esta se trata de una aplicación sencilla pero que cumple con el propósito deseado.

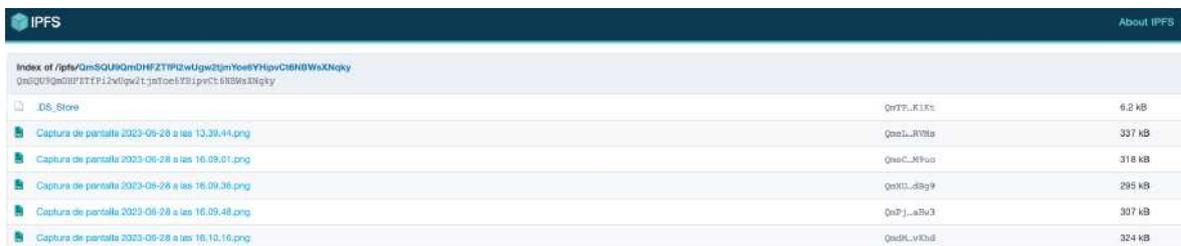
En la red IPFS, a cada elemento se le atribuye un CID (Content Identifier) el cual referencia de manera única y segura el contenido. Este CID se ha utilizado para referenciar la información dentro del sistema.



*Figura 17 - Interfaz de usuario de Pinata*



*Figura 18 - Fichero con información de los inmuebles subido a IPFS*



*Figura 19 - Fichero con las imágenes subido a IPFS*

### 5.2.4 HARDHAT

La aplicación HardHat se ha utilizado a lo largo de todo el desarrollo tanto para realizar las pruebas de los diferentes contratos inteligentes como para lanzar una Blockchain local en el equipo que es con lo que se llevan a cabo las pruebas de la aplicación.

Hardhat ha permitido crear 10 cuentas de prueba con 10.000 ETH cada una para realizar las pruebas técnicas pertinentes y dar viabilidad al sistema en un contexto académico, así como realizar las transacciones ilustrativas.

## Capítulo 6. ANÁLISIS DE RESULTADOS

Atendiendo a los objetivos comentados en la sección 4.2 del proyecto:

- Se ha conseguido desarrollar un contrato (RealEstate.sol) que genere los NFT inmobiliarios y otro que gestione la lógica de compraventa (Fondo.sol) satisfactoriamente.
- Se ha conseguido crear una estructura de compraventa con más de dos agentes de forma que las transacciones se realizan de manera segura y fiable.
- La interfaz obtenida es ciertamente atractiva y minimalista, sin información innecesaria y está adaptada para las distintas plataformas en las que se puede consumir esta página web de manera que cualquiera, de un simple vistazo es capaz de utilizarla y llevar a cabo transacciones prácticamente cualquier usuario independientemente de su nivel de dominio de la tecnología Blockchain.
- Se ha elaborado correctamente una red Blockchain de pruebas donde se ha comprobado el correcto funcionamiento de los contratos y de la red en si gracias a un entorno profesional de desarrollo en Ethereum como es HardHat.

A continuación, en las pruebas realizadas al contrato utilizando HardHat en la Figura 20, se observa como todas las funciones sometidas a la prueba funcionan según lo esperado, desde la actualización de los valores de propiedad y cantidades de ETH depositadas y enviadas.

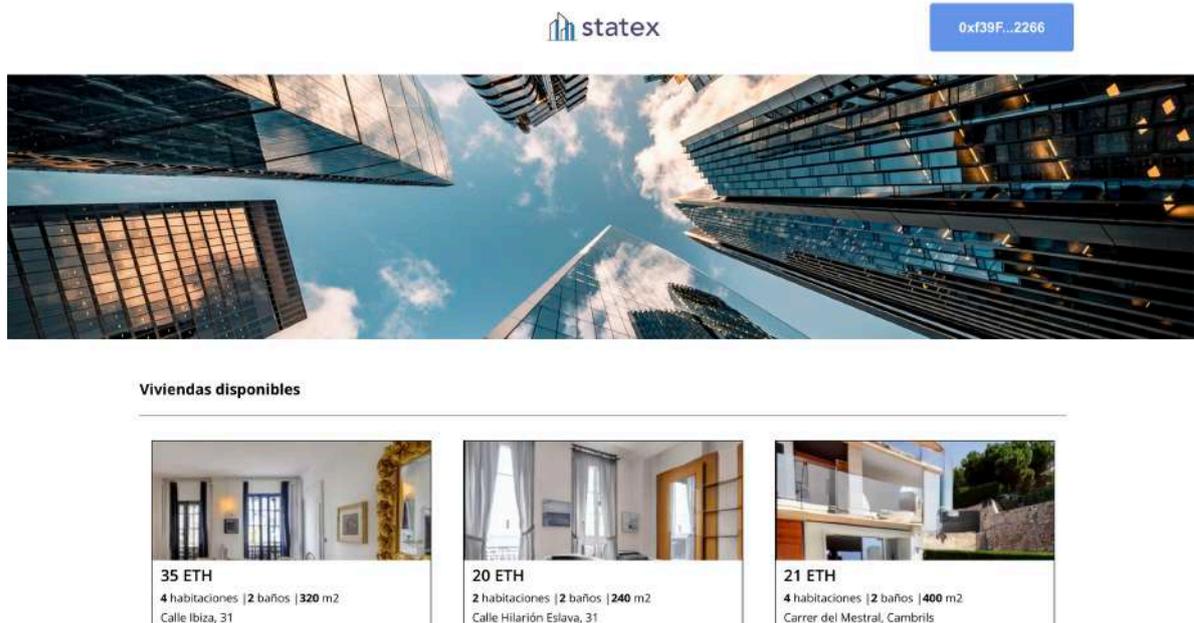
```

Contrato de fondo de garantía
Lanzamiento (deploy.js)
  ✓ Devuelve dirección NFT
  ✓ Devuelve vendedor
  ✓ Devuelve inspector
  ✓ Devuelve prestanista
Listado
  ✓ Actualiza
  ✓ Devuelve vendedor
  ✓ Devuelve el precio de compra
  ✓ Devuelve valor fondo
  ✓ Nueva propiedad
Depósito
  ✓ Actualiza el balance
Inspección
  ✓ Actualiza estatus
Aprobación
  ✓ Actualiza estatus
Venta
  ✓ Actualiza propiedad
  ✓ Actualiza balance
14 passing (2s)

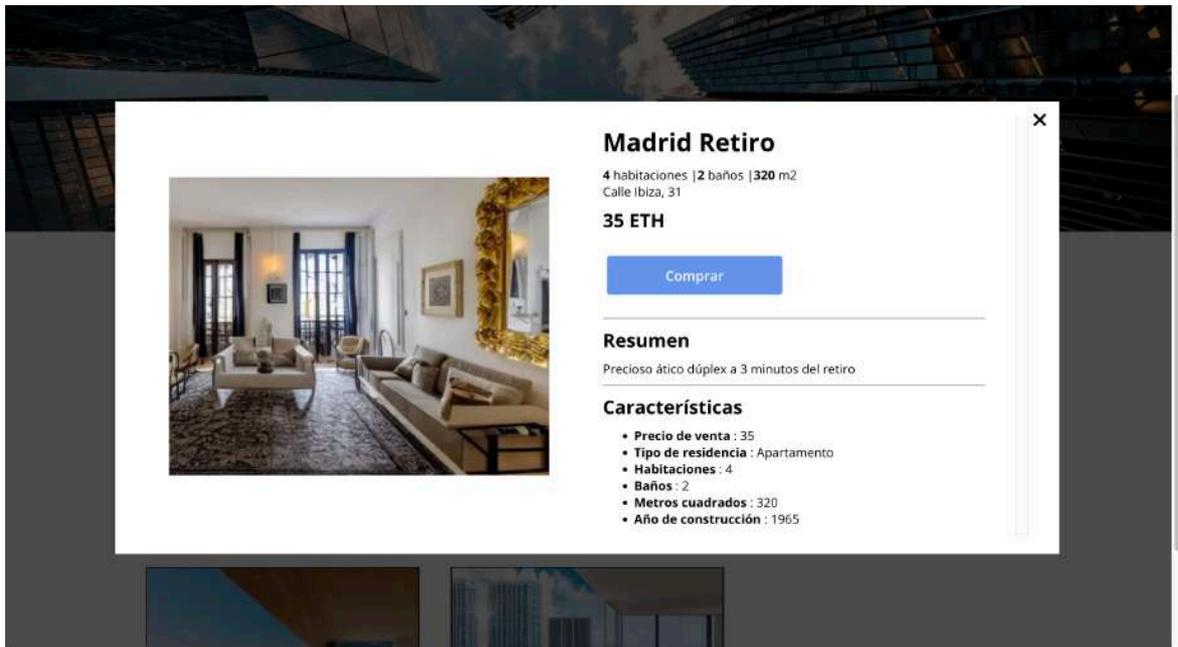
```

*Figura 20 - Test contrato Fondo.sol*

La aplicación terminada y con su interfaz finalizada se puede ver en la Figura 21 y en la Figura 22



*Figura 21 - Aspecto final aplicación*



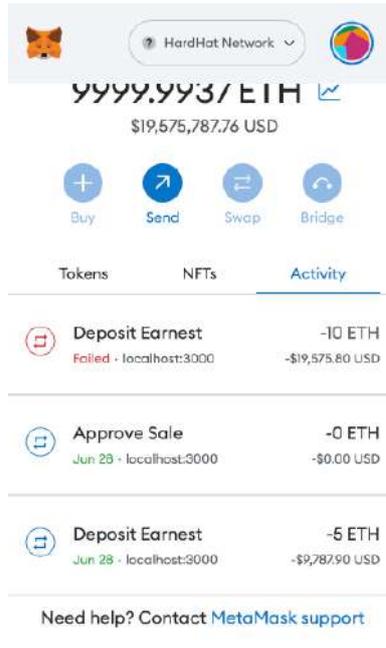
*Figura 22 - Aspecto inmuebles listados*

Como se puede ver, el aspecto es muy simple, se ha decidido además llamar al proyecto StateX, para darle un nombre comercial.

En el ANEXO II: Manual de usuario se explica con más detalle el funcionamiento de la aplicación por parte del usuario.

Con vistas a ilustrar los resultados satisfactorios del desarrollo, se ha ejecutado una transacción de ejemplo en la red con un inmueble valorado en 5 ETH. Como se puede ver en la Figura 23, se ha ejecutado con éxito la transacción aprobándose la venta tras las confirmaciones pertinentes.

Asimismo, en la misma Figura 23 se ha ejecutado una negativa por parte de los validadores y se observa cómo se ha negado el depósito de ETH en el fondo.



*Figura 23 - Pruebas transacciones*

## **Capítulo 7. CONCLUSIONES Y TRABAJOS FUTUROS**

En su conjunto se podría decir que se han conseguido los objetivos esperados con el desarrollo del Trabajo Fin de Grado prácticamente en su totalidad, se ha revisado el estado actual de la tecnología en cuestión, el del mercado inmobiliario y las soluciones Blockchain existentes.

En cuanto a los costes, el proyecto ha demostrado que tiene un potencial muy grande de crecimiento y de generar rentabilidades elevadas. Como se ha comentado en la sección 4.4.4, es probable que, teniendo en cuenta que la aplicación no se limita al territorio español, en el primer año genere rentabilidades sin un desembolso inicial realmente significativo.

Precisamente este contexto sin fronteras, internacional, que nos brindan las nuevas tecnologías es un activo muy atractivo del proyecto, y es que, si bien es cierto que cada país cuenta con su legislación y regulaciones propias complicando la posible expansión, la parte técnica sería trivial.

Toda la información de la aplicación es pública en la Blockchain, anónima y está protegida del fraude.

Como se ha expuesto con anterioridad, se han cubierto los principales objetivos del Trabajo Fin de Grado, no obstante, cabe destacar que hay una ambiciosa funcionalidad que no ha sido posible implementarla con éxito, esta es la tokenización de los inmuebles en partes alícuotas para poder gestionar la propiedad por parte de varios inversores. Tras numerosas pruebas, finalmente no fue posible desarrollar esta funcionalidad sin fallos y de manera estable, por lo que es una de las mejoras a tener en cuenta de cara al desarrollo futuro y posibles mejoras de la aplicación.

Tras consultar con un grupo de personas familiarizadas con la tecnología y con las empresas emergentes y con las propias conclusiones del autor, se han llegado a las siguientes conclusiones en cuanto a Statex y sus posibles mejoras y avances futuros:

- Entorno legal: En el contexto de una nueva empresa, es muy importante contar con cierta robustez legal. Aunque el mundo Blockchain es relativamente nuevo y cuenta con carencias legislativas, en los últimos años se han producido avances significativos particularmente en el sector inmobiliario en España. Estas mejoras legales crean una corriente de optimismo que hace ver con buenos ojos la inclusión en este mercado. Sin embargo, el ámbito legal es el principal impedimento para la expansión internacional de la aplicación.
- Completa descentralización: Si bien es cierto que la aplicación hace uso de una tecnología completamente descentralizada como es la Blockchain, dado que el proceso de compraventa de un inmueble es algo que conlleva siempre una alta suma económica y ha de estar muy supervisado, se ha elaborado un proceso de compraventa que involucra a dos terceras personas, un supervisor y un inspector. Estas personas serían empleados de la aplicación que tendría que dar el visto bueno a la operación. Una mejora futura sería explorar la viabilidad de eliminar esta escasa dependencia de la empresa y si fuera un proceso con posibilidades de ser tan seguro como lo era hasta el momento.
- Elaboración de una criptomoneda propia: Esta posibilidad de mejora podría suponer un gran avance y beneficios para la aplicación, aparte se podría controlar su precio refiriéndola al dólar o a otra moneda de curso legal (creando una stablecoin) para regular la volatilidad de las criptomonedas involucradas en el proceso.
- Nueva red Blockchain: Si bien es cierto que Ethereum es la red más popular a la hora de crear contratos inteligentes, existen muchas otras posibilidades que podrían mejorar las características de la aplicación. Un ejemplo de lo anterior sería la red de Polkadot [49]. Esta red es muy interesante en el contexto de aplicaciones descentralizadas, ya que ofrece unas comisiones muy bajas comparadas con las de Ethereum, una gran capacidad de escalabilidad y además actúa como un internet de redes Blockchain, haciendo que múltiples redes diferentes puedan comunicarse entre sí, lo cual abre un nuevo abanico de posibilidades.



## Capítulo 8. BIBLIOGRAFÍA

- [1] MedRec, «Home,» [En línea]. Available: <https://medrec-m.com/>.
- [2] IBM, «IBM Supply Chain Intelligence Suite: Food Trust,» [En línea]. Available: <https://www.ibm.com/es-es/products/supply-chain-intelligence-suite/food-trust>.
- [3] M. Segura, «Tokenización de inmuebles: factores a tener en cuenta,» [En línea]. Available: <https://www.tokeniza.es/tokenizacion-de-inmuebles-factores-a-tener-en-cuenta/>.
- [4] H. Fernández, «La historia de Internet y su impacto en la economía moderna,» [En línea]. Available: <https://economyatic.com/diccionario-tecnologico/historia-de-internet/>.
- [5] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» [En línea]. Available: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://bitcoin.org/bitcoin.pdf>.
- [6] V. Buterin, «Ethereum Whitepaper,» [En línea]. Available: <https://ethereum.org/en/whitepaper/>.
- [7] B. Santander, «¿Qué es “blockchain”?,» [En línea]. Available: <https://www.santander.com/es/stories/blockchain-que-es>.
- [8] Bit2Me, «¿Qué es un Nodo Ethereum 2.0?,» [En línea]. Available: <https://academy.bit2me.com/que-es-un-nodo-ethereum-2-0/#:~:text=Actualmente%2C%20la%20red%20Ethereum,supera%20los%2020%20mil%20nodos..>
- [9] C. Toppazzini, «Blockchain: qué es la descentralización y qué hay que saber para aprovechar las posibilidades que ofrece,» [En línea]. Available:

<https://www.a24.com/crypto/blockchain-que-es-la-descentralizacion-y-que-hay-que-saber-aprovechar-las-posibilidades-que-ofrece-n1081251>.

[10 Banco Santander, «Smart contracts, ¿qué son y para qué sirven?,» [En línea]. Available:  
] <https://www.santander.com/es/stories/smart-contracts>.

[11 Solidity, «Solidity Home,» [En línea]. Available: <https://soliditylang.org/>.  
]

[12 React, «React, pagina de inicio,» [En línea]. Available: <https://es.react.dev/>.  
]

[13 Node.js, «About,» [En línea]. Available: <https://nodejs.org/es/about>.  
]

[14 NPM, «About,» [En línea]. Available: <https://docs.npmjs.com/about-npm>.  
]

[15 Hardhat, «Documentation,» [En línea]. Available: <https://hardhat.org/docs>.  
]

[16 OpenZeppelin, «Documentation,» [En línea]. Available: <https://docs.openzeppelin.com/>.  
]

[17 Metamask, «Developer documentation,» [En línea]. Available: <https://docs.metamask.io/>.  
]

[18 Microsoft, «VS Code,» [En línea]. Available: <https://code.visualstudio.com/>.  
]

[19 IPFS, «IPFS Docs,» [En línea]. Available: <https://docs.ipfs.tech/>.  
]

- [20 Pinata, «About,» [En línea]. Available: <https://www.pinata.cloud/about>.  
]
- [21 El Mundo, «Qué es un NFT y cómo funciona,» [En línea]. Available:  
] <https://www.elmundo.es/como/2022/03/10/6229eb5c21efa072618b4578.html>.
- [22 J. P. Ponnán, «ESTÁNDAR DE TOKEN NO FUNGIBLE ERC-721,» [En línea]. Available:  
] <https://ethereum.org/es/developers/docs/standards/tokens/erc-721/>.
- [23 Himanshi, «Cryptographic Hash Functions in Blockchain,» [En línea]. Available:  
] <https://www.shiksha.com/online-courses/articles/cryptographic-hash-functions-in-blockchain/>.
- [24 A. López, «Criptografía: Qué son los algoritmos hash y para qué se utilizan,» [En línea].  
] Available: <https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-hash/>.
- [25 ByBit, «Dirección de blockchain,» [En línea]. Available:  
] <https://learn.bybit.com/es/glossary/definition-blockchain-address/>.
- [26 Iberdrola, «'Smart contracts': contratos inteligentes para formalizar acuerdos en la era  
] digital,» [En línea]. Available: <https://www.iberdrola.com/innovacion/smart-contracts>.
- [27 bit2me, «Top 5 de Lenguajes de Programación de Smart Contracts,» [En línea]. Available:  
] <https://academy.bit2me.com/top-5-de-lenguajes-de-programacion-de-smart-contracts/>.
- [28 F. Ast, «Entendiendo los Protocolos de Consenso de Blockchain,» [En línea]. Available:  
] <https://medium.com/astec/entendiendo-los-protocolos-de-consenso-de-blockchain-4858c71722d2>.
- [29 Plain Concepts, «¿Qué es la tokenización? | Claves para entenderlo,» [En línea]. Available:  
] <https://www.plainconcepts.com/es/tokenizacion/>.

- [30 L. Alejandro, «¿Qué es la inversión inmobiliaria? tipos de inversores e inversiones según riesgos y rendimientos,» [En línea]. Available: <https://moovemag.com/2020/12/que-es-la-inversion-inmobiliaria-tipos-de-inversores-e-inversiones-segun-riesgos-y-rendimientos/>.
- [31 KPMG, «¿Recuperación o reconstrucción? Así será el Real Estate en 2022,» [En línea]. Available: <https://www.tendencias.kpmg.es/2022/01/recuperacion-reconstruccion-asi-sera-real-estate-2022/>.
- [32 Expansión, «PIB de España - Producto Interior Bruto,» [En línea]. Available: <https://datosmacro.expansion.com/pib/espana>.
- [33 Fotocasa, «¿Cuánto se tarda en España en comprar una vivienda? - (c) 2023 Adevinta, en caso de que redistribuyas o difundas nuestro contenido protegido, recuerda que debes citarnos.,» [En línea]. Available: <https://www.fotocasa.es/fotocasa-life/compraventa/cuanto-se-tarda-en-espana-en-comprar-una-vivienda/>.
- [34 Idealista, «Cuánta comisión cobra una inmobiliaria por la venta de una casa en 2022,» [En línea]. Available: <https://www.idealista.com/news/inmobiliario/vivienda/2022/04/20/796078-cuanta-comision-cobra-una-inmobiliaria-por-la-venta-de-una-casa-en-2022>.
- [35 Ministerio de Justicia, «Página principal,» [En línea]. Available: <https://www.mjusticia.gob.es/en>.
- [36 Colegio de Registradores de España, «Inicio,» [En línea]. Available: <https://www.registradores.org/>.
- [37 Agencia Tributaria, «Sede electrónica,» [En línea]. Available: <https://sede.agenciatributaria.gob.es/>.

[38 Propy, «Propy,» [En línea]. Available: <https://propy.com/>.

]

[39 B. Miller, «Vermont City, Real Estate Startup Try Out Blockchain for Recording Property Transactions,» [En línea]. Available: <https://www.govtech.com/biz/vermont-city-real-estate-startup-try-out-blockchain-for-recording-property-transactions.html>.

[40 RealT, «RealT,» [En línea]. Available: <https://realt.co/>.

]

[41 Reental, «Reental,» [En línea]. Available: <https://www.reental.co/en/>.

]

[42 J. Montoriol Garriga, «Sector inmobiliario español: balance 2022 y perspectivas 2023,» [En línea]. Available: <https://www.caixabankresearch.com/es/analisis-sectorial/inmobiliario/sector-inmobiliario-espanol-balance-2022-y-perspectivas-2023>.

[43 M. Villoria, «La corrupción en España: rasgos y causas esenciales,» [En línea]. Available: <https://journals.openedition.org/ccec/5949>.

[44 A. Stsepanets, «Modelo de cascada (Waterfall): qué es y cuándo conviene usarlo,» [En línea]. Available: <https://blog.ganttpro.com/es/metodologia-de-cascada/#:~:text=El%20modelo%20de%20cascada%20es,el%20art%C3%ADculo%20de%20Winston%20W..>

[45 Pinata, «Pricing,» [En línea]. Available: <https://www.pinata.cloud/pricing>.

]

[46 Talent, «Salario medio para Programador en España, 2023,» [En línea]. Available: <https://es.talent.com/salary?job=programador>.

[47 Ministerio de transportes, movilidad y agenda urbana, «Transacciones inmobiliarias (compraventa),» [En línea]. Available: <https://apps.fomento.gob.es/BoletinOnline2/?nivel=2&orden=34000000>.

[48 UniSwap, «UniSwap,» [En línea]. Available: <https://uniswap.org/>.

]

[49 Polkadot, «Polkadot,» [En línea]. Available: <https://polkadot.network/>.

]

[50 Agencia tributaria, [En línea]. Available:

] [https://sede.agenciatributaria.gob.es/Sede/ayuda/manuales-videos-folletos/manuales-practicos/folleto-actividades-economicas/3-impuesto-sobre-renta-personas-fisicas/3\\_5-estimacion-directa-simplificada/3\\_5\\_4-tabla-amortizacion-simplificada.html](https://sede.agenciatributaria.gob.es/Sede/ayuda/manuales-videos-folletos/manuales-practicos/folleto-actividades-economicas/3-impuesto-sobre-renta-personas-fisicas/3_5-estimacion-directa-simplificada/3_5_4-tabla-amortizacion-simplificada.html) .

# ANEXO I: ALINEACIÓN DEL PROYECTO CON LOS ODS

Los Objetivos de Desarrollo Sostenible (ODS) son un conjunto de 17 metas globales establecidos por la Organización de las Naciones Unidas (ONU) en 2015 con el objetivo de abordar las principales preocupaciones mundiales en materia de desarrollo. Los ODS se basan en la idea de que el desarrollo económico, social y ambiental son interdependientes y deben abordarse de manera equilibrada y son los que se muestran en la Figura 24 - ODS. Fuente: ONU.



*Figura 24 - ODS. Fuente: ONU*

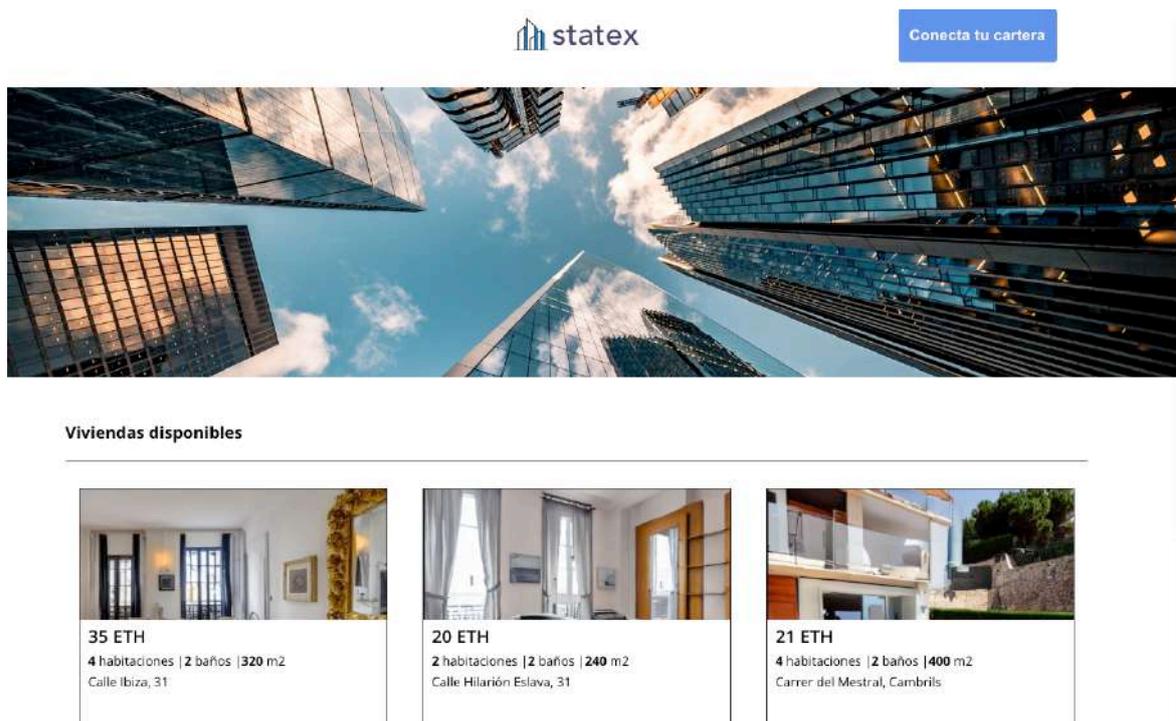
En concreto, en este Trabajo Fin de Grado aborda el objetivo 8 y 9.

- Objetivo 8: Trabajo decente y crecimiento económico. En este proyecto se trata de potenciar el acceso al mercado inmobiliario haciendo que este pueda crecer eliminando sus barreras de entrada y eliminando intermediarios.

- Objetivo 9: Industria, innovación e infraestructura. Se busca innovar en una industria clave en la economía de los países como es el mercado inmobiliario utilizando tecnologías de vanguardia.

## ANEXO II: MANUAL DE USUARIO

La aplicación requiere para su utilización tener una cartera de MetaMask activa en la red Ethereum ya que sin ella, simplemente podrá visualizar la página pero no realizar ninguna otra operación más allá de la visualización.



*Figura 25 - Statex sin conectar la cartera*

Una vez pulsado el botón de ‘Conecta tu cartera’ que puede verse en la Figura 25, el usuario podrá comprobar como la primera vez que realiza el proceso, ha de seleccionar en MetaMask la cuenta con la que desea acceder a la aplicación. Una vez hecho este primer trámite, no será necesario más adelante y se conectará automáticamente.



0xf39F...2266

Figura 26 - Apariencia de usuario con la cartera conectada

Manteniendo el principio del minimalismo en el diseño, nada más se accede a la web se pueden observar los inmuebles listados y algunas de sus características más relevantes, así como una pequeña imagen del mismo como se ve en la Figura 27.

#### Viviendas disponibles

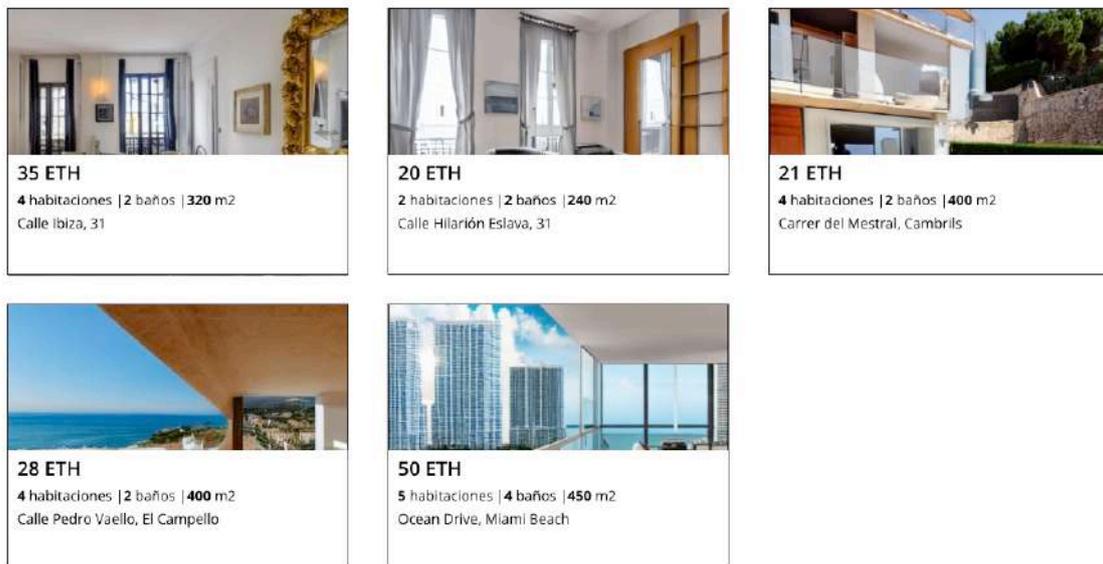
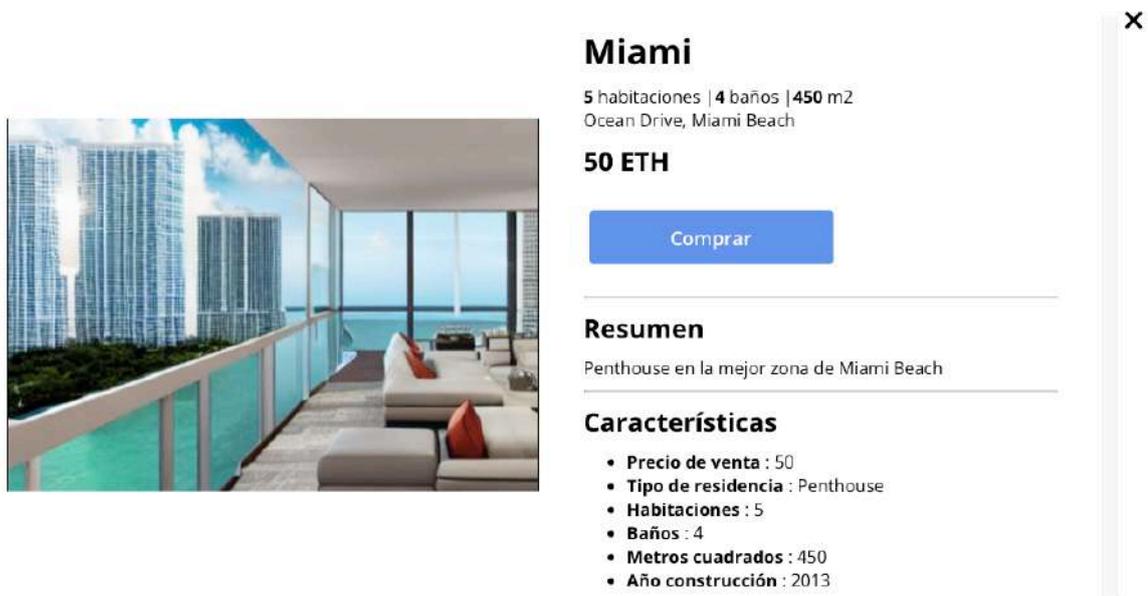


Figura 27 - Apartado viviendas disponibles Statex

Cuando el usuario pincha en cada uno de esos inmuebles, se abre una ventana donde se ven los bienes raíces más en detalle incluyendo todas sus características principales. Esto se ilustra en la Figura 28



**Miami**

5 habitaciones | 4 baños | 450 m2  
Ocean Drive, Miami Beach

**50 ETH**

Comprar

**Resumen**

Penthouse en la mejor zona de Miami Beach

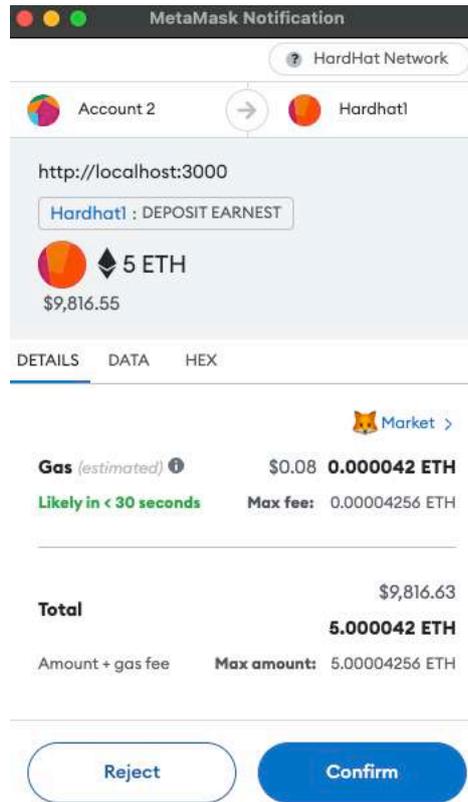
**Características**

- Precio de venta : 50
- Tipo de residencia : Penthouse
- Habitaciones : 5
- Baños : 4
- Metros cuadrados : 450
- Año construcción : 2013

*Figura 28 - Ejemplo de inmueble listado*

Cuando el cliente de la aplicación se decide por una de las viviendas, solo tiene que pulsar el botón comprar, automáticamente se lanza la transacción a la cadena de bloques como se muestra en la Figura 29 y se retiran sus fondos a la espera de que sea aprobada por los agentes internos de la aplicación.

Una vez es aprobada, se realiza el proceso de cambio de dueño y de liberación de los activos y se corrobora con el mensaje en MetaMask de venta aprobada de la Figura 30.



*Figura 29 - Transacción ejemplo*

	<b>Approve Sale</b> Jun 28 · localhost:3000	<b>-0 ETH</b> -\$0.00 USD
	<b>Deposit Earnest</b> Jun 28 · localhost:3000	<b>-5 ETH</b> -\$9,787.90 USD

*Figura 30 - Venta aprobada*

## ANEXO III: MANUAL DE INSTALACIÓN

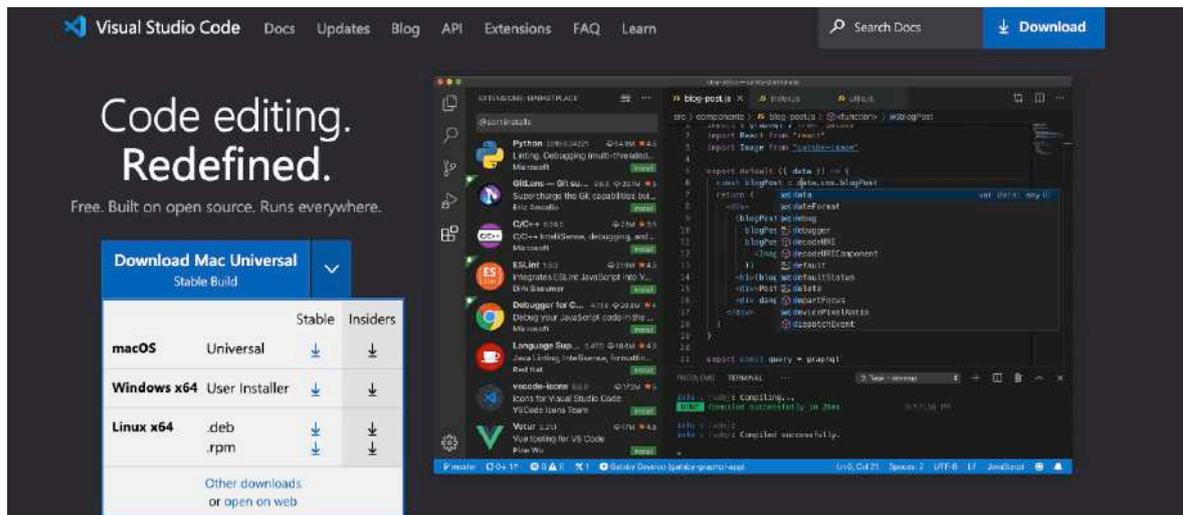
En primer lugar, el usuario deberá descargar la aplicación Node.js, la cual podrá descargarse en su página web [50] donde se verá una pantalla como la de la Figura 31. Pulsando en la versión 18.16.1 LTS se descargará la versión a utilizar.



Figura 31 - Instalación Node.js

Posteriormente, se instalará VS Code, cabe destacar que no es un requerimiento obligatorio para el funcionamiento de la aplicación, sin embargo, es la mejor opción de cara a simplificar y unificar el proceso en todos los sistemas operativos debido a su opción de poder usar terminales integradas.

Para ello, el usuario se dirigirá a la web oficial de VS Code [18] y se pulsará el link de descarga que sea necesario para cada sistema como se ve en la Figura 32.



*Figura 32 - Instalación de VS Code*

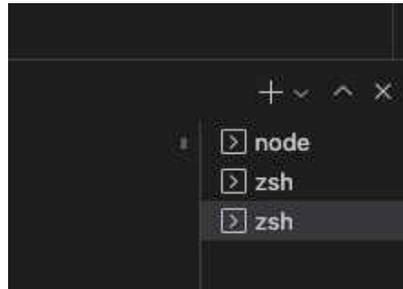
En este punto, se abrirá la carpeta del proyecto Statex con VS Code, dentro del explorador de archivos de la propia aplicación.



*Figura 33 - Abrir terminal VS Code*

En las opciones, se pulsa Terminal y Nuevo terminal en la barra superior (Ver Figura 33). Una vez en el terminal, se ejecutará el comando: `npm install`, para instalar las dependencias de npm. Cuando finalice el proceso de instalación, se lanza la red de prueba en Hardhat, con el comando: `npx hardhat node`. Esto desplegará la Blockchain local.

En este momento es cuando se realiza el lanzamiento de los contratos o *deploy*. Se abre una nueva terminal haciendo una pulsación el icono de '+' que se puede ver en la Figura 34.



*Figura 34 - Nueva terminal*

En este nuevo terminal lanzaremos el archivo `deploy.js` con el comando: `npx hardhat run ./scripts/deploy.js --network localhost`

Finalmente, solo quedar lanzar la aplicación en el *front-end*, para ello utilizaremos las dependencias npm con el comando: `npm run start`.