



GRADO EN INGENIERÍA EN TECNOLOGÍAS DE
TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

**Aplicación de las Tecnologías
Blockchain y Smart Contract en el
ámbito legal de Sucesiones y
Herencias**

Autor: Manuel Mora de Amarillas

Director: Atilano Fernández-Pacheco Sánchez-Migallón

Co-Director: José Luis Gahete Díaz

Madrid

Agosto 2020

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

**APLICACIÓN DE LAS TECNOLOGÍAS BLOCKCHAIN Y SMART CONTRACT EN
EL ÁMBITO LEGAL DE SUCESIONES Y HERENCIAS**

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

curso académico 2019/20 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.: Manuel Mora de Amarillas

Fecha: 21/08/2020

Autorizada la entrega del proyecto

LOS DIRECTORES DEL PROYECTO



Fdo.: Atilano Fernández-Pacheco Sánchez-Migallón

Fecha: 22/08/2020



Fdo.: José Luis Gahete Díaz

Fecha: 22/08/2020



GRADO EN INGENIERÍA EN TECNOLOGÍAS DE
TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

**Aplicación de las Tecnologías
Blockchain y Smart Contract en el
ámbito legal de Sucesiones y
Herencias**

Autor: Manuel Mora de Amarillas

Director: Atilano Fernández-Pacheco Sánchez-Migallón

Co-Director: José Luis Gahete Díaz

Madrid

Agosto 2020

Agradecimientos

Agradecer a mis padres, por su paciencia y apoyo, que me han animado siempre para conseguir los objetivos que me proponga, y de los que continúo todos los días aprendiendo a actuar ante las distintas situaciones en la vida.

A mi hermana Concha, compañera de profesión y de la que he aprendido la constancia, esfuerzo y tenacidad en los estudios y el trabajo.

A mis abuelas, que siempre se alegran de cada logro que consigo como si fuera de ellas. Mis abuelos, que, aunque no están me siguen cuidando los que más. Mis tíos, pacientes y que me tratan como si fuera su hijo. Y demás familia.

Agradecer en especial a Miguel de Amarillas Sevilla, letrado de profesión y mi tío, por estar siempre abierto y disponible para resolverme cualquier duda legal de este proyecto.

Agradecer a mis directores de proyecto, Atilano y José Luis, por permitirme realizar este Trabajo Fin de Grado bajo su supervisión, animarme a llevar a cabo esta idea y haberme guiado durante el transcurso del proyecto con paciencia y comprensión ante las adversidades que han surgido durante este curso.

A mis amigos, que siempre están ahí, por su lealtad y ánimos en los momentos difíciles sin dudar en ningún momento.

Y finalmente, a mis profesores y compañeros de la universidad, que han formado parte de mi día a día estos últimos años y han contribuido a mi formación personal y académica.

APLICACIÓN DE LAS TECNOLOGÍAS BLOCKCHAIN Y SMART CONTRACT EN EL ÁMBITO LEGAL DE SUCESIONES Y HERENCIAS

Autor: Mora de Amarillas, Manuel.

Director: Fernández-Pacheco Sánchez-Migallón, Atilano.

Co-Director: Gahete Díaz, José Luis.

Entidad Colaboradora: ICAI – Universidad Pontificia Comillas

RESUMEN DEL PROYECTO

En la actualidad, existen multitud de gestiones legales cuyo paradigma para realizarlas es el mismo que hace más de un siglo, como la elaboración de testamentos y el proceso de herencia, ambos complejos, largos y en muchas ocasiones costosos, debido a los intermediarios que garantizan la seguridad durante su tramitación, tales como el notario. Además, sin ayuda legal, estos procesos pueden complicarse.

Este Trabajo Fin de Grado abarca el diseño, desarrollo e implementación de una aplicación web basada en las tecnologías de Blockchain y Smart Contract, con el fin de demostrar que actualmente existe la tecnología necesaria para crear un nuevo modelo basado en ésta, que permita tener mayor control, transparencia y seguridad que el modelo tradicional.

Palabras clave: Blockchain, Smart Contract, Testamento, Herencia.

1. Introducción

Blockchain es una tecnología que da sus inicios junto con la aparición del proyecto Bitcoin en 2008 en el artículo [1] de la mano de Satoshi Nakamoto. En él, se propone el uso de redes descentralizadas *peer to peer* (P2P) junto con algoritmos de consenso entre nodos y algoritmos asimétricos (sistema de clave pública y firma digital). La idea principal de ese proyecto era utilizar la tecnología planteada para realizar transacciones bancarias con criptodivisas, eliminando a los bancos como intermediarios de las operaciones y ocupándose del control de ellas la red descentralizada.

La tecnología de dicho proyecto se extrapola dando lugar a los Smart Contracts, los cuales permiten realizar transacciones administrativas de otros ámbitos distintos al bancario. La tecnología de Blockchain y Smart Contracts permite abordar casuísticas como trazabilidad de pólizas de seguros o transacciones jurídicas como el caso planteado en este Trabajo Fin de Grado, herencias y sucesiones, sustituyendo la confiabilidad que se otorga a terceras personas en el proceso, como los notarios, y mejorando la seguridad y transparencia durante el proceso gracias a las características propias de estas tecnologías.

2. Definición del proyecto

En este Trabajo Fin de Grado se diseña un nuevo modelo del proceso de escritura de testamentos (ver CC 667 en [2]) y de herencia mediante el desarrollo de una aplicación web descentralizada apoyada sobre la tecnología Blockchain y Smart Contract con el fin de que los usuarios puedan confeccionar sus propios testamentos que podrán ser ejecutados automáticamente cuando los clientes fenezcan, dando lugar al reparto de los bienes inmuebles según lo establecido en las últimas voluntades del difunto.

Para el desarrollo de la aplicación es necesario el diseño y desarrollo de un Registro de la Propiedad, donde se inscriben los bienes raíces, y un Registro Civil, que permita el registro de Certificados Médicos de Defunción. Ambos estarán basados también en la tecnología Blockchain y Smart Contract y podrán comunicarse con la lógica de la aplicación para llevar a cabo los procesos de testamentaría y herencia.

Así mismo, al final de este proyecto se valida el funcionamiento de la aplicación desarrollada en una red simulada de Ethereum [3], red de Blockchain que permite ejecución de Smart Contracts.

3. Descripción del modelo

Para el desarrollo de este proyecto es necesario una infraestructura donde poder implantar la aplicación web descentralizada. Esta infraestructura puede verse en la *Figura 1*.

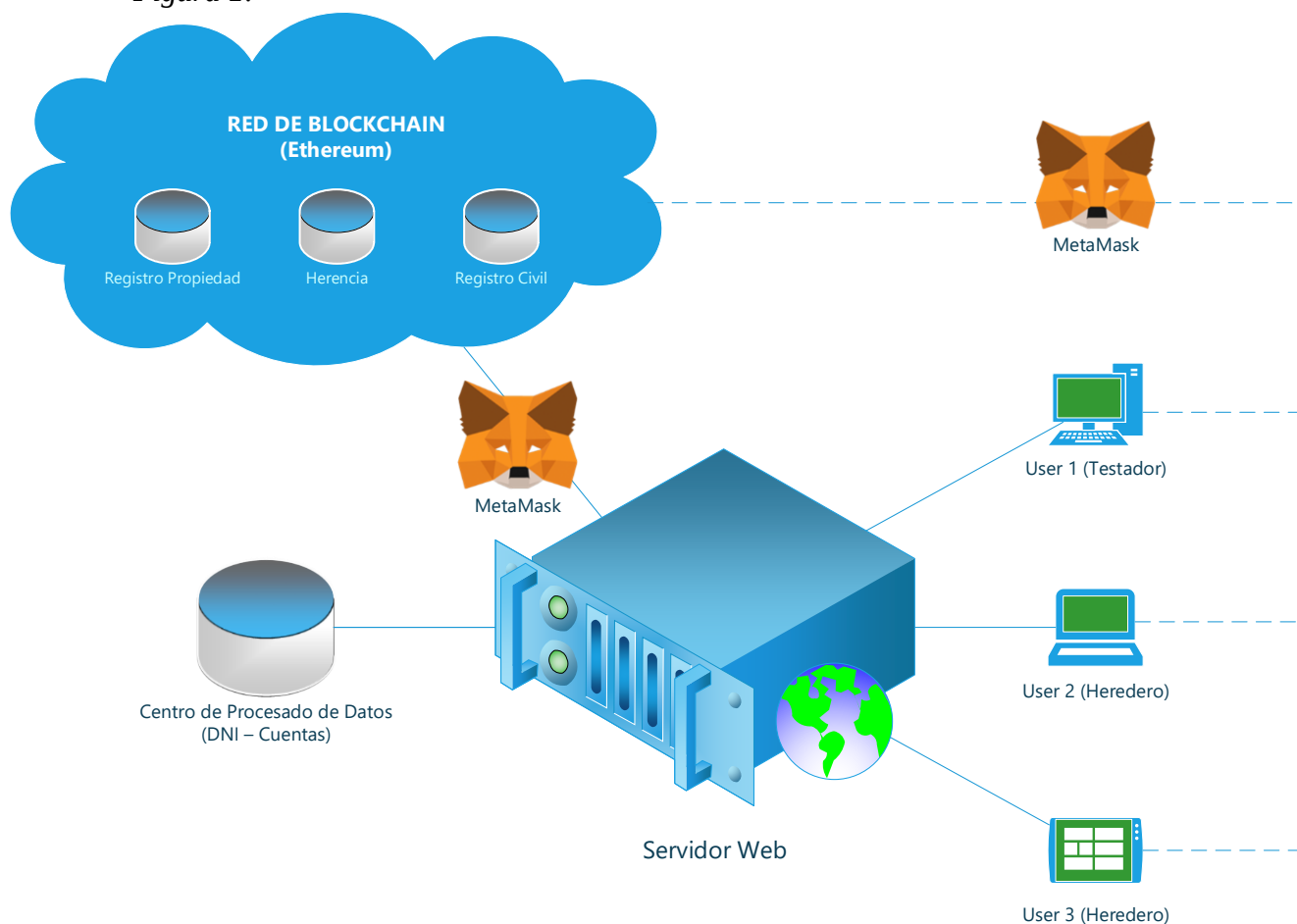


Figura 1. Diagrama de la arquitectura del sistema

La infraestructura consta de cuatro elementos:

- **Red de Blockchain (Ethereum):** En ella reside el *back-end*, formado por los Smart Contracts del Registro Civil, Registro de la Propiedad y la lógica del proceso de herencia.
- **Centro de Proceso de Datos:** Consiste en una base de datos con el registro de los DNIs de los usuarios asociados a una cuenta de la red de blockchain.
- **Servidor web:** Donde se almacena el *front-end* de la aplicación que permite a los usuarios interactuar con ella.
- **Otros elementos:** En la infraestructura hay otros elementos como los usuarios, que podrán ser también parte de la propia red de blockchain, y MetaMask, que se trata de un monedero de criptomonedas a través del cual los usuarios y la web interactúa con la red de blockchain.

Para llevar a cabo la implementación de la aplicación web descentralizada, en primer lugar, se han desarrollado los Smart Contracts (*back-end*) que contienen la lógica de la aplicación. A continuación, se ha procedido con el desarrollo del *front-end* y diseño de la base de datos del Centro de Proceso de Datos para, posteriormente, establecer una comunicación con el *back-end* a través de *web3.js*. Finalmente se ha procedido al despliegue del *front-end* en un servidor, a la simulación de una red de blockchain Ethereum para el despliegue *back-end* y se ha comprobado el correcto funcionamiento de la aplicación web descentralizada.

A continuación, en la *Figura 2* se muestra un diagrama de flujo del proceso de desarrollo e implantación de la aplicación desarrollada.

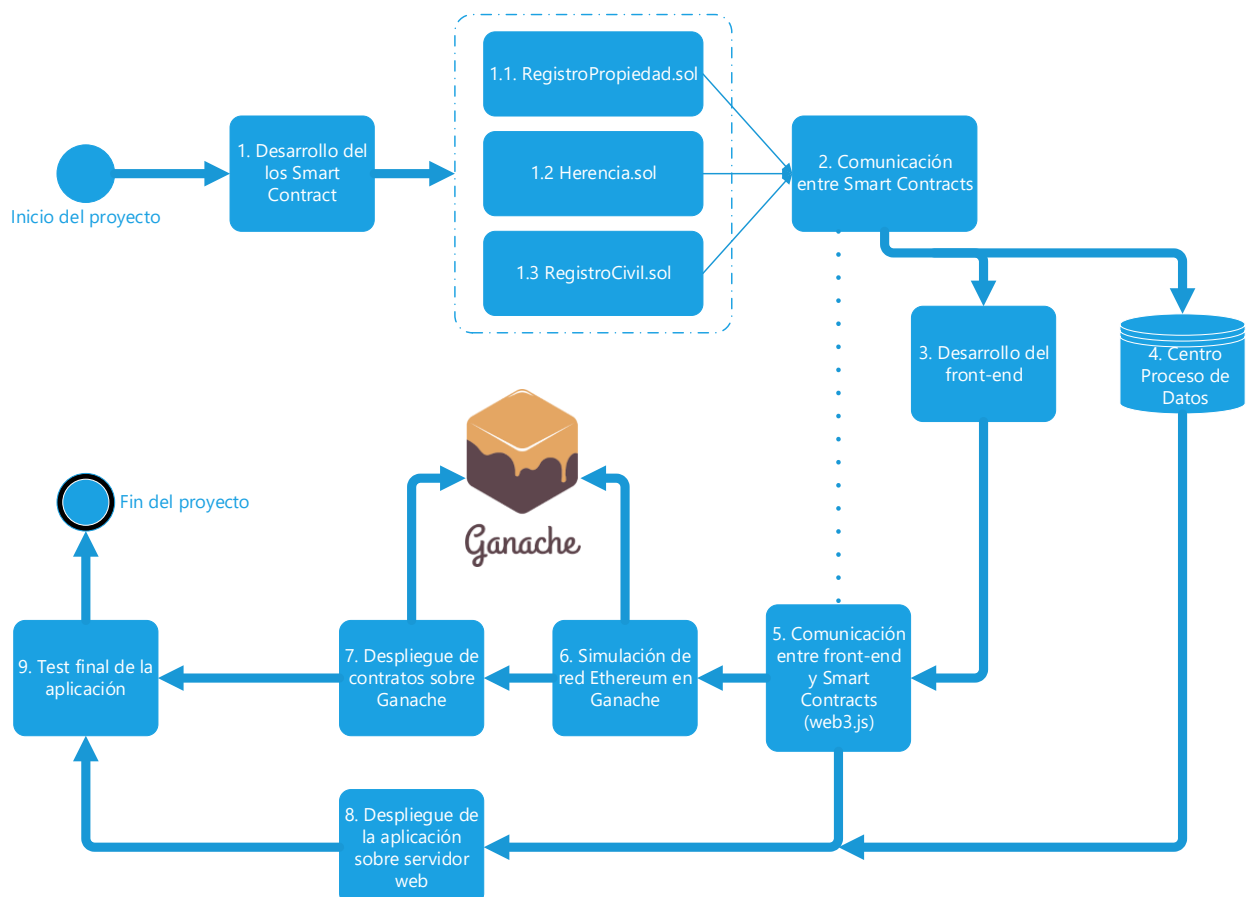


Figura 2. Diagrama de flujo del desarrollo de la aplicación web

4. Resultados

El resultado de este Trabajo Fin de Grado es la implementación de una aplicación web descentralizada que permita la escritura de testamentos por los propios usuarios y llevar a cabo el proceso de herencia.

La aplicación web desarrollada se caracteriza por ser:

- Funcional: Sustituyendo al modelo tradicional.
- Dinámica: Generando contenido según las interacciones del usuario con la aplicación sin requerir de navegación entre pantallas estáticas.
- La aplicación consta de dos vistas:
 - Vista del usuario: Donde se podrá crear testamentos, consultarlos y consultar trámites pendientes. Véase *Figura 3. Captura de vista de un usuario*.
 - Vista del administrador: Donde se podrá administrar el Registro de la Propiedad, Registro Civil y ejecutar testamentos. Véase *Figura 4. Captura de vista del administrador*.

HERENCIA

NOMBRELUCIA

CUENTA ACTUAL0xd747a0fa5d3bb9d39127bceaa1f73383f18f

DNI04082003L

Crear Testamento

Introduzca su fecha de nacimiento:
04/08/2003Comenzar Testamento

Testamento creado con id:11289660858653219800358161328320537388637064355590285072861804453252130411420

Introduzca numero de herederos: 1

Propietario (dni) 110121983S

Porcentaje 100

Introduzca numero de herederos: 2

Propietario (dni) 110121983S

Porcentaje 40

Propietario (dni) 223091980A

Porcentaje 60

Firmar Testamento

Se está realizando el testamento

Trámites pendientes

Usuario fallecido: CRISTINA (DNI: 18121985C)

Cuenta del usuario: 0xd09a112DAD9B326B88C84C58b314CA4Fccc838463

Id testamento: 99327612663062764484370705614696440997313456685710162459070959038195949484255

Usuario fallecido: JUAN (DNI: 10031980J)

Cuenta del usuario: 0x8277cAef1735cB9486A0C38F79F7938cE4230f5f

Id testamento: 30914741005829671642519655492758364500150805472441042043427505648299846193794

Fincas a heredar y porcentaje

Idiufir: 9999: 60%

Aceptar

Rechazar

Aceptado

Pendiente

Certificado de Últimas Voluntades:

Id CUV52071488529374516351802143686454834689784304583090914601038826925917018002478

Nombre de la personaLUCIA

DNI de la persona04082003L

Cuenta de la persona0xd747a0fa5d3bb9d39127bceaa1f73383f18f

Fecha NacimientoLunes 4/8/2003

Testamentos

Id Testamento

Testamento seleccionado:

Id Testamento:15729937481500977773872904299150047976792055134749775347638463225650814643695

Id CUV:52071488529374516351802143686454834689784304583090914601038826925917018002478

Cuenta de la persona0xd747a0fa5d3bb9d39127bceaa1f73383f18f

Fecha de creación del testamento:Viernes 21/8/2020

Estado del testamentoSin Ejecutar

HerederosSusana (dni: 10121983S), Alberto (dni: 23091980A),

Cuentas herederos0xe57DDFC9c30225819d3904C962834649724b403f0xe4D5120220a610577e6b35f5F7938Ec8A4e3726

Decisión de herederos(true/false)false,false

Resumen Traspasos

Nº Traspaso	Idiufir	Herederos	Porcentajes
1	7777	0xe57DDFC9c30225819d3904C962834649724b403f	100
2	4444	0xe57DDFC9c30225819d3904C962834649724b403f	60
		0xe4D5120220a610577e6b35f5F7938Ec8A4e3726	40

Traspaso nº 2

Idiufir7777

PropietariosSusana (dni: 10121983S)

Propietarios (Cuentas):0xe57DDFC9c30225819d3904C962834649724b403f

Porcentajes100

Propietarios rechazan:

Propietarios rechazan (Cuentas)

Propietarios rechazan

Propietarios aceptados:

Propietarios aceptados (Cuentas)

Propietarios aceptados

Figura 3. Captura de vista de un usuario

Registro de la Propiedad

NOMBRE MINISTERIO
CUENTA ACTUAL 0xa6a2dc761eedce3ed8dd274f10c2cb67ef18b5c4
DNI 0000000M

Buscar Finca

Idufir a buscar

Añadir finca

Idufir
Municipio
Nº Finca
Metros2
Tipo
Nº Propietarios
Propietario (DNI) Porcentaje propiedad

Registro Civil

Buscar Certificado Médico de Defunción

Buscar por cuenta
 Buscar por DNI

Añadir Certificado Médico de Defunción

Nombre
Primer apellido
Segundo apellido
Fecha nacimiento dd/mm/aaaa
Fecha defuncion dd/mm/aaaa
DNI de la persona

Ejecutar Testamento

DNI del difunto

Figura 4. Captura de vista del administrador

5. Conclusiones

Este Trabajo Fin de Grado ha conseguido los objetivos marcados desarrollando una aplicación web descentralizada para implementar un nuevo modelo de los procesos de testamentaría y herencia que cumplen las mismas funciones que el modelo tradicional, aportando mayor seguridad y transparencia sin necesidad de intermediarios.

Este Trabajo abre la posibilidad a otros trabajos para implantar un mayor desarrollo de la aplicación, con la incorporación en mayor medida de la legislación vigente sobre derecho de sucesiones o implantando procesos *Batch* para automatizar el modelo.

Así mismo, este Trabajo Fin de Grado puede dar lugar a nuevas líneas de investigación sobre la aplicación de Blockchain y los Smart Contracts en otros ámbitos que requieren de procesos seguros sin la necesidad de intermediarios.

6. Referencias

- [1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." Acceso: Jul. 30, 2020. [Online]. Disponible: www.bitcoin.org.
- [2] España. Ministerio de Gracia y Justicia, *Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. 1889*.
- [3] "Qué es Ethereum (ETH) | Bit2Me Academy." <https://academy.bit2me.com/que-es-ethereum-eth-criptomoneda/> (Acceso: Aug. 21, 2020).

APPLICATION OF BLOCKCHAIN AND SMART CONTRACT TECHNOLOGIES TO THE LEGAL FIELD FOR SUCCESSIONS AND INHERITANCES

Author: Mora de Amarillas, Manuel.

Supervisor: Fernández-Pacheco Sánchez-Migallón, Atilano.

Co-supervisor: Gahete Díaz, José Luis.

Collaborating Entity: ICAI – Universidad Pontificia Comillas.

ABSTRACT

Currently, there are many legal processes which have been kept unchanged since from more than one century ago. One of them is the preparation of wills and inheritance process, both are large, complex and in many times expensive due to the cost of intermediaries to ensure the security of the process like the public notary. In addition, the process can become more complex without legal support.

This Final Degree Project covers the design, development and implementation of a web application based on Blockchain and Smart Contract technologies. The objective is to demonstrate that the needed technology is already available to create a new model based on it to allow more control, transparency, and security of the legacy model.

Keywords: Blockchain, Smart Contract, Will, Inheritance.

1. Introduction

Blockchain is a technology, which was born with Satoshi Nakamoto's Bitcoin project in 2008 (see article [1]). In that project it is proposed the usage of decentralized networks *peer to peer* (P2P) jointly with algorithms of consensus between peers and asymmetric algorithms (public key and digital signature system). The main idea was to use that technology to perform banking transactions with cryptocurrency, removing banks as intermediaries and while decentralized network takes the control.

That technology is extrapolated to create Smart Contracts, which allow performing other administrative activities out of the banking scope. Blockchain and Smart Contract technologies allow tracing insurance policies or legal transactions like the case of this Final Degree Project, inheritances and successions, replacing public notaries and improving security and transparency of the process thanks to these technologies characteristics.

2. Project Definition

In this Final Degree Project, it is designed a new process to prepare wills (see CC 667 in [2]) and inheritance through decentralized application based on Blockchain and Smart Contract technologies. This will allow users to create their own wills which can be automatically executed when users pass away leading to the split of the real estate according to the will.

To the development of the application, it will be necessary the design and development of Public Registry of Property, to record the real estate, and Civil Registry to record Medical Certificates of Death. Both are also based on the Blockchain and Smart Contract technology and can communicate with the application to perform the will and inheritance processes.

Also, at the end of this project, the functioning of the application is validating in a simulated Ethereum [3] network. This is a Blockchain network that allows execution of Smart Contracts.

3. Model Description

The architecture to implement the decentralized application can be seen in *Figure 1*.

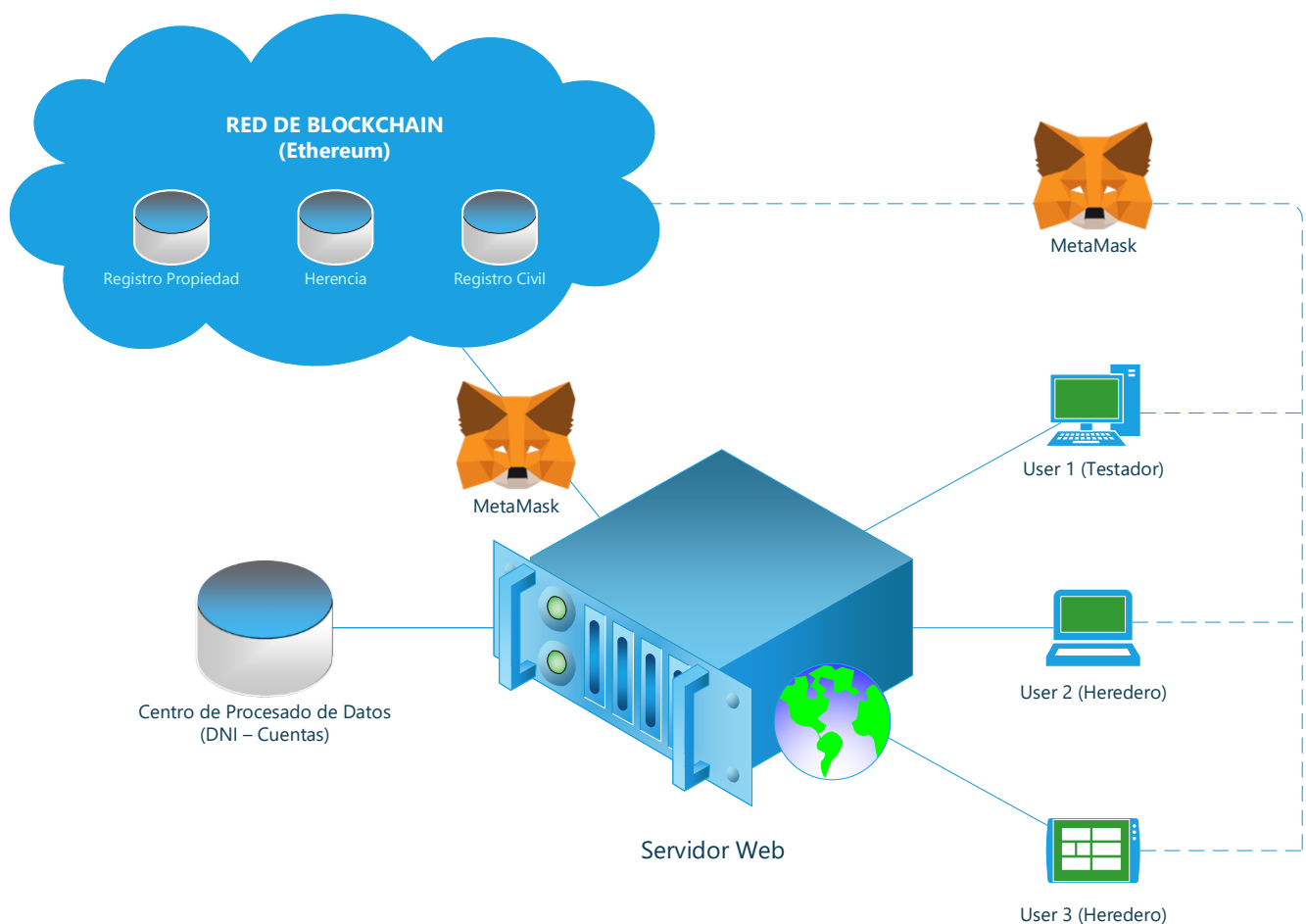


Figure 1. System Architecture Diagram

The system architecture is composed by the following four elements:

- **Blockchain Network (Ethereum):** Here is located the *back-end*, including the Smart Contracts of Civil Registry, Public Registry of Property and the inheritance process logic.
- **Data Processing Centre:** It is a data base to record the IDs (DNIs) of the users associated to a blockchain network account.

- **Web Server:** Where the application *front-end* is stored allowing users interact with it.
- **Other Elements:** In the system architecture there are other elements like users, which can be also part of the Blockchain network, and MetaMask, which is a cryptocurrency wallet through which users and web interact with the Blockchain network.

To implement the decentralized application, first, Smart Contracts (back-end) containing the logic of the application have been developed. After, the *front-end* and data base of the Data Processing Centre have been developed to further communicate to the *back-end* through the *web3.js*. Finally, the *front-end* has been deployed in a web server, the simulation of the Ethereum Blockchain network to deploy the *back-end* in it and it has been checked the proper functioning of the decentralized application.

The *Figure 2* shows flow diagram of the development and implementation process of the application.

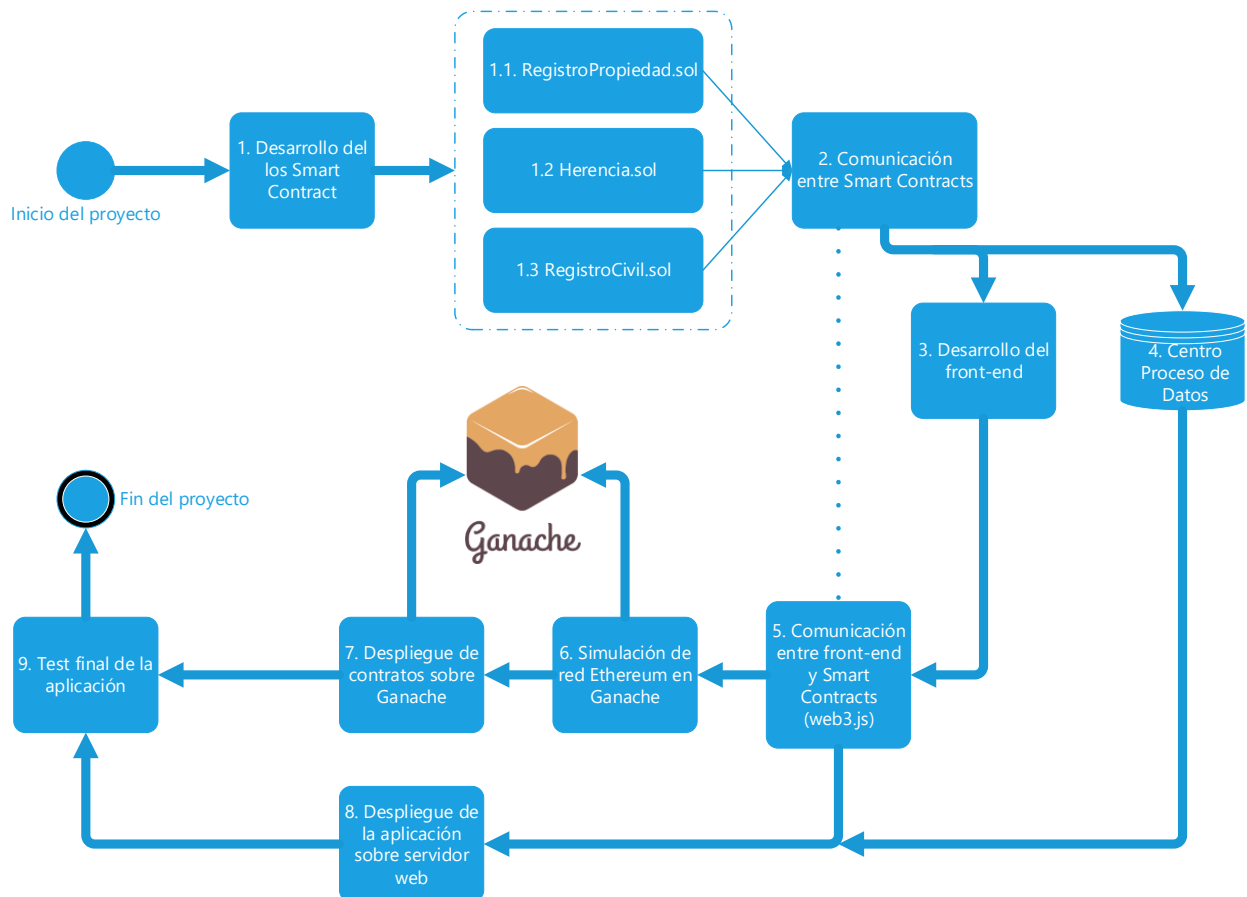


Figure 2. Flow Diagram of the Development and Implementation process

4. Results

The result of this Final Degree Project is the implementation of a decentralized application that allow users the preparation of their own wills and performing the inheritance process.

The characteristics of the developed application are:

- Functional: Replacing the legacy model.
- Dynamic: Allowing users interact with the application without navigating through static screens.
- The application is composed by two views:
 - User view: Where wills can be created and consulted, as well as formalities can be consulted. See *Figure 3. User View*.
 - Administrator view: Where Public Property Register and Civil Register could be managed, as well as execute wills. See *Figure 4. Administrator View*.

HERENCIA

NOMBRE

LUCIA

CUENTA ACTUAL

0x67d7a0fa5b5d3bb9d39127bc5a1f73383f18f

DNI

04082003L

Crear Testamento

Introduzca su fecha de nacimiento:

04/09/2003

Comenzar Testamento

Testamento creado con id:

11289660858653219800358161328320537388637064355590285072861804453252130411420

Introduzca numero de herederos:

1

Porcentaje:

100

Propietario (dni)

1

10121983S

Madrid

Piso

Porcentaje:

100

Introduzca numero de herederos:

2

Porcentaje:

40

Propietario (dni)

1

10121983S

Porcentaje:

60

Propietario (dni)

2

23091980A

Firmar Testamento

Se está realizando el testamento

Trámites pendientes

Usuario fallecido:

CRISTINA (DNI: 18121985C)

Cuenta del usuario:

0x09a7f2d2ad9b320b88c84c58b314ca4fcca838463

Id testamento:

99327612663062764484370705614696440997313456685710162459070959038195949484255

Usuario fallecido:

JUAN (DNI: 10031980J)

Cuenta del usuario:

0x8277cAcf1735cB9486A0C38F79F7938cE42303f

Id testamento:

30914741005829671642519655492758364500150805472441042043427505648299846193794

Fincas a heredar y porcentaje

Idiufir: 9999: 60%

Acceptar

Rechazar

Pendiente

Certificado de Últimas Voluntades:

Id CUV

52071488529374516351802143686454834689784304583090914601038826925917018002478

Nombre de la persona

LUCIA

DNI de la persona

04082003L

Cuenta de la persona

0x67D7a0FA5b5d3bb9D39127bcEAA1F73383F18F

Fecha Nacimiento

Lunes 4 8 2003

Testamentos

Testamento nº 1

Testamento nº 2

Id Testamento

Testamento seleccionado:

Id Testamento:

1572993748150097773872904299150047976792055134749775347638463225650814643695

Id CUV:

52071488529374516351802143686454834689784304583090914601038826925917018002478

Cuenta de la persona

0x67D7a0FA5b5d3bb9D39127bcEAA1F73383F18F

Fecha de creación del testamento

Viernes 21 8 2020

Estado del testamento

Sin Ejecutar

Herederos

Susana (dni: 10121983S), Alberto (dni: 23091980A)

Cuentas herederos

0xE57DDFC9c30225819d3904c962834649724b403f,0xE4D5120220a610577eE6b35f5F7938Ee8A4e3726

Decisión de heredero(true/false)

false,false

Resumen Traspasos

Nº Traspaso

Idiufir

Herederos

Porcentajes

1

0xE57DDFC9c30225819d3904c962834649724b403f

100

2

0xE4D5120220a610577eE6b35f5F7938Ee8A4e3726

40

Traspaso nº 2

Idiufir

7777

Propietarios:

Susana (dni: 10121983S)

Propietarios (Cuentas):

0xE57DDFC9c30225819d3904c962834649724b403f

Porcentajes

100

Propietarios rechazan:

Propietarios rechazan (Cuentas)

Propietarios rechazan

Propietarios aceptados:

Propietarios aceptados (Cuentas)

Propietarios aceptados

Figure 3. User View

Registro de la Propiedad

NOMBRE MINISTERIO
CUENTA ACTUAL 0xa6a2dc761eedce3ed8dd274f10c2cb67ef18b5c4
DNI 0000000M

Buscar Finca

Añadir finca

Idufir
Municipio
Nº Finca
Metros2
Tipo
Nº Propietarios
Propietario (DNI) Porcentaje propiedad

Registro Civil

Buscar Certificado Médico de Defunción

Añadir Certificado Médico de Defunción

Nombre
Primer apellido
Segundo apellido
Fecha nacimiento
Fecha defuncion
DNI de la persona

Ejecutar Testamento

DNI del difunto

Figure 4. Administrator View

5. Conclusions

This Final Degree Project has reached the stablished objectives by developing a decentralized application to implement a new model to perform the will and inheritance processes, with the same functions than the legacy model bringing more security and transparency without intermediaries.

This Project opens the possibility to other works to further develop the application by deeper incorporating the current regulations on the inheritance laws and implementing *Batch* processes to automate the model.

Moreover, this Final Degree Project may lead to new research lines about the use of Blockchain and Smart Contracts technologies on other areas requiring secure processes without the need of intermediaries.

6. References

- [1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System." Accessed: Jul. 30, 2020. [Online]. Disponible: www.bitcoin.org.
- [2] España. Ministerio de Gracia y Justicia, *Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil. 1889*.
- [3] "Qué es Ethereum (ETH) | Bit2Me Academy." <https://academy.bit2me.com/que-es-ethereum-eth-criptomoneda/> (Accessed: Aug. 21, 2020).

Índice de la memoria

Capítulo 1. Introducción	11
Capítulo 2. Descripción de las Tecnologías.....	13
2.1 Blockchain.....	13
2.2 Ethereum	14
2.3 Smart Contract.....	14
2.3.1 Lenguajes de programación de Smart Contracts	15
2.3.1.1 Solidity	15
2.3.1.2 Viper.....	15
2.3.1.3 Otros Lenguajes	15
2.4 Tecnología Web	16
2.4.1 HyperText Transfer Protocol (HTTP).....	16
2.4.2 Lenguajes de programación web.....	16
2.4.2.1 HyperText Markup Language (HTML)	16
2.4.2.2 Cascading Style Sheets (CSS).....	17
2.4.2.3 JavaScript	17
2.4.2.4 PHP	17
2.4.3 Bases de datos (BBDD)	17
2.4.3.1 MySQL.....	18
2.4.3.2 phpMyAdmin	18
2.5 Web3.js.....	18
2.6 Otras herramientas usadas	19
2.6.1 Ganache.....	19
2.6.2 Remix IDE	19
2.6.3 MetaMask	20
2.6.4 ATOM	20
2.6.5 Google Chrome	20
2.6.6 MiniWeb Server.....	20
2.6.7 WampServer	21
Capítulo 3. Estado de la Cuestión	23
3.1 Blockchain.....	23

3.1.1	Funcionamiento de Blockchain	23
3.1.2	Algoritmos de consenso	25
3.1.2.1	Proof of Work (PoW)	26
3.1.2.2	Otros algoritmos de consenso	27
3.1.3	Estado actual de Blockchain y Criptomonedas	28
3.1.4	Aplicaciones descentralizadas y proyectos apoyados sobre Ethereum.....	31
3.2	Estado de la cuestión del proceso de Testamentaría y Herencia.	32
3.3	Proyectos de testamentaría y herencias basados en blockchain	34
Capítulo 4.	Definición del Trabajo	35
4.1	Justificación.....	35
4.2	Objetivos	36
4.3	Metodología.....	37
4.4	Estimación Económica	39
4.4.1	Recursos materiales.....	39
4.4.2	Recursos humanos.....	41
4.4.3	Presupuesto total.....	42
Capítulo 5.	Modelo Desarrollado	43
5.1	Análisis del modelo	43
5.1.1	Análisis del proceso de elaboración de testamentos	43
5.1.2	Análisis del proceso de herencia	47
5.1.3	Requisitos de diseño obtenidos.....	50
5.2	Diseño.....	53
5.2.1	Diseño de arquitectura	53
5.2.2	Diagramas de casos de uso	55
5.2.3	Estructura de datos principal	58
5.2.4	Diagrama de clases	60
5.2.5	Diagramas de secuencia.....	62
5.2.6	Diseño del front-end	69
5.3	Implementación	72
Capítulo 6.	Análisis de Resultados.....	77
Capítulo 7.	Conclusiones y Trabajos Futuros.....	89

Capítulo 8. Bibliografía.....	93
ANEXO I: Alineación del proyecto con los ODS	97
ANEXO II: Manual de instalación.....	101
A II. 1 Configuración de ganache	101
A II. 2 Configuración de los servicios WampServer	103
A II. 2.1 Configuración de phpMyAdmin y MySQL	104
A II. 2.2 Configuración del servidor apache y hosts virtuales	105
A II. 3 Despliegue de los contratos desde Remix en Ganache.....	108
A II. 4 Configuración de comunicación entre back-end y front-end	112
A II. 5 Instalación y configuración de MetaMask	113
Anexo III: Manual del usuario.....	119
A III.1 Inicio de la aplicación	119
A II. 2 tfg.ministerio.com	121
A III. 2.1 Registro de la Propiedad	121
A III. 2.1.1 Consulta de una propiedad o inmueble.....	121
A III. 2.1.2 Registro de una propiedad o inmueble	122
A III. 2.2 Registro Civil	123
A III. 2.2.1 Consulta de un Certificado Médico de Defunción.....	123
A III. 2.2.2 Registro de un Certificado Médico de Defunción	125
A III. 2.2.3 Ejecución de un Testamento.....	126
A II. 3 tfg.mitestamento.com	127
A III. 3.1 Creación de Testamentos	127
A III. 3.2 Consulta del Certificado de Últimas Voluntades y Testamentos	130
A III. 3.2.1 Consulta de un Certificado de Últimas Voluntades.....	130
A III. 3.2.2 Consulta de un Testamento	131
A III. 3.2.3 Consulta de un Traspaso.....	131
A III. 3.3 Trámite pendientes.....	133
A III. 3.3.1 Consulta de un Trámite pendiente	133
A III. 3.3.2 Aceptar/renunciar a una herencia	133

Índice de ilustraciones

Ilustración 1. Funcionamiento de Blockchain	25
Ilustración 2. Evolución de la expedición de BTC respecto al número de bloques minados y recompensas por bloque minado	30
Ilustración 3. Diagrama de Gantt con las tareas del proyecto	37
Ilustración 4. Panel Kanban del backlog del proyecto	38
Ilustración 5. Proceso de elaboración de Testamento con modelo tradicional.....	45
Ilustración 6. Proceso de elaboración de Testamento con el modelo propuesto	46
Ilustración 7. Proceso de Herencia con el modelo tradicional	48
Ilustración 8. Proceso de Herencia con el nuevo modelo propuesto	50
Ilustración 9. Diagrama de la arquitectura del sistema.....	54
Ilustración 10. Diagrama de casos de uso del actor Cliente	56
Ilustración 11. Diagrama de casos de uso del actor Ministerio	57
Ilustración 12. Diagrama de estructura de datos.....	59
Ilustración 13. Diagrama de clases del modelo propuesto	61
Ilustración 14. Diagrama de secuencia para la creación de fincas	62
Ilustración 15. Diagrama de secuencia de consulta de fincas.....	63
Ilustración 16. Diagrama de secuencia de la creación de un CMD	63
Ilustración 17. Diagrama de secuencia de la consulta de un CMD	64
Ilustración 18. Diagrama de secuencia de escritura de Testamento	65
Ilustración 19. Diagrama de secuencia de la consulta de Testamentos	66
Ilustración 20. Diagrama de secuencia del proceso de herencia (I)	68
Ilustración 21. Diagrama de secuencia del proceso de herencia (II)	69
Ilustración 22. Diagrama estructural de la pantalla del usuario Ministerio.....	70
Ilustración 23. Diagrama estructural de la pantalla del usuario Cliente.....	71
Ilustración 24. Diagrama de flujo del proceso de desarrollo de la aplicación web	72
Ilustración 25. Captura de IDE Remix en el proceso de desarrollo	73
Ilustración 26. Captura del administrador de base de datos phpMyAdmin durante el desarrollo	74

Ilustración 27. Captura de Ganache simulando una red descentralizada durante el desarrollo	75
Ilustración 28. Captura durante despliegue de contratos y pruebas de integración.....	78
Ilustración 29. Capturas del front-end de la aplicación durante el desarrollo	79
Ilustración 30. Consultas de datos realizadas por línea de comandos con sentencias SQL	80
Ilustración 31. Resolución de una promesa solicitando un CMD a la red de blockchain ...	81
Ilustración 32. Resolución de una promesa solicitando información de una finca a la red de blockchain.....	81
Ilustración 33. Detalle de la información del usuario conectado a la aplicación	82
Ilustración 34. Captura de la vista del usuario Ministerio	83
Ilustración 35. Administración del Registro Civil.....	84
Ilustración 36. Administración del Registro de la Propiedad.....	84
Ilustración 37. Captura de la vista del usuario Cliente	85
Ilustración 38. Proceso de escritura de Testamento (Superior), Trámites pendientes (Inferior)	86
Ilustración 39. Vista de los datos mostrados del CUV de un cliente.....	87
Ilustración 40. Objetivos de Desarrollo Sostenible	97
Ilustración 41. Configuración de Ganache (a).....	101
Ilustración 42. Selección de una red existente en Ganache (b)	102
Ilustración 43. Aplicación Ganache en ejecución simulando una red	102
Ilustración 44. Inicio de la aplicación WampServer.....	103
Ilustración 45. Servicios de WampServer	103
Ilustración 46. Entorno de phpMyAdmin.....	104
Ilustración 47. Importación de base de datos	104
Ilustración 48. BBSS importada	105
Ilustración 49. Contenido del archivo "hosts"	106
Ilustración 50. Contenido del archivo "httpd-vhosts.conf"	106
Ilustración 51. Contenido de la carpeta "www"	107
Ilustración 52. Reinicio de servicios	107
Ilustración 53. Dominio de la aplicación.....	107

Ilustración 54. Remix IDE.....	108
Ilustración 55. Menú “Deploy & run transactions”.....	108
Ilustración 56. Configuración de conexión con red de Ganache	109
Ilustración 57. Cuentas de Ganache visualizadas en Remix IDE.....	109
Ilustración 58. Despliegue de contratos.....	110
Ilustración 59. Transacciones realizadas durante el despliegue	110
Ilustración 60. Detalle de un contrato desplegado en Remix IDE.....	111
Ilustración 61. Métodos para configurar direcciones de las interfaces.....	112
Ilustración 62. Configuración de variables que definen direcciones de contratos	112
Ilustración 63. Pantalla de inicio en MetaMask	113
Ilustración 64. Selección inicial en MetaMask.....	113
Ilustración 65. Creación de contraseña para la cartera	114
Ilustración 66. Frase secreta de backup	114
Ilustración 67. Confirmación de frase secreta	115
Ilustración 68. Pantalla inicial de MetaMask	115
Ilustración 69. Configuración de red Ganache en MetaMask	116
Ilustración 70. Detalle de información de la cuenta index 2 de Ganache	116
Ilustración 71. Importación de una cuenta en MetaMask.....	117
Ilustración 72. Captura de la aplicación en funcionamiento	117
Ilustración 73. Vista de "tfg.ministerio.com"	120
Ilustración 74. Vista de "tfg.ministerio.com"	120
Ilustración 75. Consulta realizada de una finca (Idufir: 9890).....	121
Ilustración 76. Introducción de datos de una finca.....	122
Ilustración 77. Introducción de datos de los propietarios de una finca	122
Ilustración 78. Confirmación de transacción del registro de una finca	123
Ilustración 79. Cuadro de búsqueda de un CMD.....	124
Ilustración 80. Búsqueda de CMD por cuenta.....	124
Ilustración 81. Búsqueda de CMD por cuenta.....	124
Ilustración 82. Registro de un nuevo CMD.....	125
Ilustración 83. Confirmación de transacción del registro de un CMD.....	125

Ilustración 84. Cuadro de ejecución de un Testamento	126
Ilustración 85. Confirmación de transacción de la ejecución de un Testamento	126
Ilustración 86. Cuadro de inicio de un Testamento	127
Ilustración 87. Confirmación de transacción de la creación de un Testamento	128
Ilustración 88. Selección del número de herederos	128
Ilustración 89. Asignación traspasos en un testamento	129
Ilustración 90. Confirmar transacción de firma de un Testamento	130
Ilustración 91. Vista de la consulta del CUV de un cliente	131
Ilustración 92. Consulta de un CUV en detalle	132
Ilustración 93. Vista de Trámites pendientes de un usuario	133
Ilustración 94. Botones aceptar/rechazar herencia	133
Ilustración 95. Confirmar transacción de Aceptar/Rechazar herencia	134
Ilustración 96. Vista de trámites de un usuario después de Aceptar una herencia	134

Índice de tablas

Tabla 1. Especificaciones de ordenador portátil.....	39
Tabla 2. Especificaciones monitor auxiliar	39
Tabla 3. Horas de trabajo.....	40
Tabla 4. Costes de recursos materiales	41
Tabla 5. Costes de recursos humanos	41
Tabla 6. Coste total del proyecto	42

Capítulo 1. INTRODUCCIÓN

En la sociedad actual, nos encontramos rodeados de dispositivos electrónicos cuya tecnología busca facilitar la vida de las personas. Somos conscientes de la ayuda que nos aporta la tecnología que usamos a nivel individual en nuestro día a día, sobre todo desde principios de este siglo, con la aparición y expansión de los dispositivos inteligentes que llevamos con nosotros y nos permite no solo realizar tareas de forma digital como consultar calendarios, agenda y demás, sino que, gracias a la infraestructura que existe, estos dispositivos forman parte de una red que permite que los dispositivos estén, y por tanto nosotros también, interconectados pudiendo usar la tecnología no solo a nivel individual sino también poder relacionarnos con otras personas, dispositivos o infraestructuras.

Sin embargo, pese al avance de la tecnología durante los últimos años, seguimos realizando tareas con el mismo paradigma que hace un siglo, un claro ejemplo de esto es la existencia de los bancos. Si es cierto que recientemente se han promocionado las transacciones y gestiones bancarias online y tanto los bancos como la tecnología se han adaptado para poder interactuar entre sí, pero, ¿Son todavía necesarios los bancos en la época en la que vivimos, con las tecnologías que existen en la actualidad?

La respuesta podemos encontrarla en proyectos como Bitcoin y la tecnología Blockchain, que proponen un nuevo modelo y paradigma para realizar transacciones bancarias sin la necesidad de una entidad o control central que supervise la actividad bancaria.

De igual forma, la aparición de Bitcoin y Blockchain plantea la posibilidad de extrapolar esta idea a otros ámbitos desarrollando la tecnología Smart Contract para aplicar el mismo paradigma que aplica Bitcoin a la banca tradicional, a otras transacciones administrativas en nuestra sociedad, las cuales son complejas y hacen uso de intermediarios para realizarse con seguridad. Algunos ejemplos son la trazabilidad de pólizas de seguros, expedientes médicos o en el ámbito legal, como es el caso de este Trabajo Fin de Grado, el proceso de herencias y sucesiones.

En este Trabajo Fin de Grado, se ha buscado investigar sobre la tecnología Blockchain y Smart Contract y su posible aplicación en el ámbito legal de sucesiones y herencias. Se ha llevado a cabo el desarrollo de una aplicación web dedicada a la realización de testamentos que podrán ser ejecutados de manera automática cuando se produce la defunción de una persona, dando lugar al reparto de bienes tal y como se había establecido en las últimas voluntades del difunto.

Actualmente según la ley en España, el proceso de elaborar un testamento y todos los trámites que se realizan desde que una persona fenece hasta que sus bienes han sido traspasados a los herederos designados o no, requieren de la figura del notario¹. Además, si los clientes tanto testadores como herederos no son letrados o expertos en este campo, es un proceso muy tedioso, el cual sin ayuda de un abogado o asesor legal puede llegar a complicarse junto con todos los costes que conlleva los trámites realizados por las administraciones y el notario.

Debido a la legislación vigente en España, se parte de la base que actualmente no se puede implantar este proyecto y su aplicación, pero el objetivo es demostrar que existe la tecnología necesaria para realizar todos los trámites y procesos descritos otorgando una confiabilidad y seguridad que garantice un proceso transparente e incorruptible evitando la intervención a traición de terceras personas en el proceso y que los testamentos puedan ser manipulados.

El interés de llevar a cabo este proyecto es disminuir el número de trámites, disminuir el coste de estos trámites y también reducir el intervalo de tiempo desde que se produce la defunción hasta que se ha terminado todo el proceso de herencia. Como consecuencia a las características propias de la tecnología Blockchain y los Smart Contracts, las figuras del notario y asesores legales en estos procesos desaparecerían y con ellos las complicaciones y costes que derivan de sus servicios.

¹ Notario: funcionario público autorizado para dar fe de los contratos, testamentos y otros actos extrajudiciales, conforma a las leyes y deja testimonio de los acontecimientos de los que es testigo. (Fuente: Real Academia Española: <https://www.rae.es/drae2001/notario>)

Capítulo 2. DESCRIPCIÓN DE LAS TECNOLOGÍAS

En este apartado se va a explicar las tecnologías usadas para llevar a cabo este trabajo fin de grado y mencionar las herramientas que se ha usado respecto a cada tecnología.

2.1 BLOCKCHAIN

Blockchain es una tecnología que consiste en un sistema o red descentralizada, la cual está formada por varios nodos y permite el almacenamiento de registro único. Sigue el esquema “peer to peer” (P2P) y en los nodos figuran todas las transacciones y operaciones que se van realizando en la red, lo que garantiza su disponibilidad.

Un sistema Blockchain se caracteriza no solo por garantizar la disponibilidad, sino también por la confiabilidad que esta red ofrece, ya que al crear múltiples copias en la red se garantiza la incorruptibilidad de los datos almacenados en esta y por tanto se evita que los datos puedan ser manipulados y modificados a traición.

El comienzo de la idea de este sistema se remonta a 2008, en el artículo [1] publicado por Satoshi Nakamoto, alias de persona o grupo de personas a las que se le atribuye la creación del protocolo de Blockchain usado para el proyecto Bitcoin. En este artículo se documenta que la tecnología Blockchain soporta el proyecto Bitcoin, que con el paso del tiempo ha dado lugar a la creación de otras criptomonedas y proyectos haciendo uso de este tipo de redes y sistemas como los Smart Contracts.

Cabe destacar que Blockchain hace uso de técnicas criptográficas para trabajar con los datos que se almacenan en ella y dotar a la red de la seguridad requerida. Hace uso tanto de algoritmos simétricos (clave única), como de algoritmos asimétricos (sistema de clave pública y firma digital). En el apartado 3.1.1 *Funcionamiento de Blockchain* se detallará el funcionamiento de esta tecnología y su estado actual.

2.2 *ETHEREUM*

Ethereum [2] se trata de una plataforma de código abierto a nivel global dedicado a aplicaciones descentralizadas. Su lanzamiento fue en 2015 con su propia criptomoneda nativa Ether (ETH), pero esta red no solo permite transacciones con criptomonedas, Ethereum es programable por lo que los desarrolladores pueden crear sus propias aplicaciones descentralizadas (Dapps) y desplegarlas en la red de Ethereum que permite beneficiarse de las ventajas de la tecnología de las criptomonedas.

Existen multitud de Dapps creadas como billeteras de criptomonedas, juegos sobre la red de blockchain, mercados descentralizados y otras muchas.

Ethereum es similar a Bitcoin con la diferencia que Bitcoin estaba orientado a realizar transacciones económicas de dicha criptomoneda mientras que Ethereum permite además ejecutar programas en su red creando Dapps que interactúan con las criptomonedas e información que estos programas almacenan en la red. Estos programas están escritos en una serie de scripts cuya lógica se ejecuta sobre una máquina virtual llamada “*Ethereum Virtual Machine*” (EVM). Cada nodo de la red dispone de una EVM que permite tanto ejecutar lógica de programación como gestionar información de cuentas de Ethereum. Por lo tanto, Ethereum almacena los datos en la blockchain y ejecuta los scripts en la EVM que se encuentra en los nodos. Los scripts que contienen la lógica de programación son conocidos como Smart Contracts y no podemos hablar de Ethereum y aplicaciones descentralizadas sin definir que es un Smart Contract.

2.3 *SMART CONTRACT*

Un Smart Contract o contrato inteligente consiste en una serie de instrucciones que se ejecutan en una red descentralizada P2P, en este caso Ethereum, y dichas instrucciones contenidas en el contrato se ejecutan cuando se cumplen una serie de condiciones.

Los Smart Contract se asemejan a los contratos que existen en un sistema legal en los países desarrollados. Según la Real Academia Española un “contrato” se define como:

1. Pacto o convenio, oral o escrito, entre partes que se obligan sobre materia o cosa determinada, y a cuyo cumplimiento pueden ser compelidas.
2. Documento que recoge las condiciones de este pacto o convenio.

Es decir, un contrato no deja de ser un conjunto de instrucciones, reglas o normas de las que se hace constar compromiso a su cumplimiento por las partes que intervienen en este. Además, un Smart Contract se define en [3] como “... aquellos contratos que se ejecutan de manera automática cuando se da alguna circunstancia que se hubiera estipulado”.

En la práctica, un Smart Contract es un script desplegado en la red blockchain donde figuran las instrucciones de programación necesarias para el fin que busca el desarrollador. Estos scripts se programan en un lenguaje creado para facilitar la programación de Smart Contract de los cuales hablamos a continuación.

2.3.1 LENGUAJES DE PROGRAMACIÓN DE SMART CONTRACTS

Actualmente existen múltiples lenguajes de programación para Smart Contracts:

2.3.1.1 Solidity

Lenguaje de programación de alto nivel que se ha usado para el desarrollo de este proyecto. Está basado en JavaScript y ha sido creado para implementar contratos inteligentes en Ethereum. Es un lenguaje similar a Python, C++ o JavaScript y funciona sobre la Máquina virtual de Ethereum (EVM). Se puede encontrar su documentación en [4].

2.3.1.2 Viper

Lenguaje de programación basado en Python cuyo objetivo es centrarse en la seguridad, simplicidad en su compilado y su auditabilidad para escribirse de una forma sencilla y natural. También funciona sobre la Máquina Virtual de Ethereum (EVM). Se puede encontrar su documentación en [5].

2.3.1.3 Otros Lenguajes

Existen otros lenguajes Para programar Smart Contracts como Python, java o C++. Todos ellos con bibliotecas o paquetes específicos para interactuar en la red de blockchain, pero los más usados específicamente son los nombrados anteriormente: Solidity y Vyper.

2.4 TECNOLOGÍA WEB

Tecnología abierta al desarrollo de páginas y aplicaciones web a las que los clientes pueden acceder como a través de la World Wide Web (WWW), a través de redes de blockchain o redes privadas.

2.4.1 HYPERTEXT TRANSFER PROTOCOL (HTTP)

Las tecnologías Web hacen uso del protocolo Hypertext Transfer Protocol [6]. Es un protocolo orientado a la capa de aplicación que permite transmitir documentos hipermedia (documentos que contienen soporte para texto, imágenes, videos...). En su origen se diseñó para la comunicación entre servidores y navegadores web, aunque con el paso del tiempo su uso se ha extendido para otros fines. También en sus comienzos estaba orientado a una conexión TCP/IP en la capa transporte, aunque actualmente también puede ser usado con otros protocolos como UDP. Existe otro protocolo derivado de este, Hypertext Transfer Protocol Secure (HTTPS), el cual se diferencia de HTTP en que este usa una conexión segura con un cifrado SSL por lo tanto permite una transferencia de datos más segura que HTTP.

2.4.2 LENGUAJES DE PROGRAMACIÓN WEB

Normalmente, las aplicaciones web constan de una parte *front-end*, parte visual de la web que se ejecuta en la propia máquina donde se está consultando la página web, y una parte de *back-end*, que es la parte de la web que se ejecuta en máquinas ajenas al cliente como servidores y contienen la lógica de la funcionalidad de la web en cuestión. En nuestro caso el *back-end* será la propia red de blockchain. A continuación, se muestran los lenguajes usados para la programación del *front-end* de la aplicación web y que se caracterizan por ser muy livianos en cuanto a peso ya que se ejecutan en la máquina del cliente y no interesa que tengan un tamaño excesivo.

2.4.2.1 HyperText Markup Language (HTML)

Lenguaje básico para la programación de páginas y aplicaciones web. Permite dar una estructura al contenido de la web y permite establecer enlaces con la misma u otras webs mediante hipervínculos. Se suele usar junto con otros lenguajes para mejorar la apariencia y

presentación como las hojas de estilo CSS o lenguajes para potenciar ciertas funcionalidades de la web como JavaScript. Documentación de HTML en [7].

2.4.2.2 Cascading Style Sheets (CSS)

Cascading Style Sheets (CSS) u hojas de estilo en cascada es un lenguaje de programación orientado al diseño gráfico que permiten mejorar la apariencia de las páginas web para que éstas no muestren simplemente texto plano estructurado. Existen herramientas, bibliotecas o *frameworks*² para facilitar la programación en este lenguaje. Algunos de los más conocidos son *Bootstrap*, *Materialize CSS*, *Zurb Foundation*, etc. Documentación de CSS en [8].

2.4.2.3 JavaScript

Es un lenguaje de programación que permite añadir funcionalidades al *front-end* de la web y cuyo código se ejecuta directamente en el navegador del cliente ya que se trata de un lenguaje compilado *Just in Time* o interpretado. Este lenguaje de programación permite que los sitios web en la actualidad sean mucho más interactivos y avanzados. Documentación de JavaScript en [9].

2.4.2.4 PHP

PHP [10] se trata de un lenguaje de código abierto para programar scripts ejecutados en el lado del servidor que pueden incrustarse en HTML. Cabe destacar que, a diferencia de JavaScript, al ser un lenguaje ejecutado en el servidor, el cliente lo único que hace es recibir el resultado de ejecutar el script o trozos de código sin que este conozca el código que subyace. En este proyecto se usará para establecer comunicación con la base de datos de la que se habla más adelante.

2.4.3 BASES DE DATOS (BBDD)

Blockchain, en cierto modo, puede funcionar como una base de datos donde se almacena información como clave valor. El único problema es que la escritura de información puede

² *Frameworks*: Consisten en módulos de software que permiten facilitar la escritura del código evitando código repetitivo y funcionalidades avanzadas complejas de programar desde cero

ser lenta ya que hay que esperar a que se realice el minado de un bloque. Existen situaciones en las que puede interesar, ya sea por la infraestructura disponible y la adaptabilidad del proyecto, como por conveniencia, usar bases de datos relacionales. En este proyecto se va a usar una base de datos para almacenar una serie de datos de los clientes que no requiere hacer uso de la red de blockchain.

2.4.3.1 MySQL

MySQL [11] se trata de un sistema de código abierto que permite crear y gestionar bases de datos mediante lenguaje de consultas estructurado SQL. Se basa en el modelo cliente-servidor, ya que los datos no tienen por qué almacenarse en el propio dispositivo del cliente como otras bases de datos, sino que la base de datos puede estar en un servidor al que se le realizan consultas. Se caracteriza por su facilidad de uso y flexibilidad, alto rendimiento y seguridad.

2.4.3.2 phpMyAdmin

Se trata de una herramienta que permite la administración de bases de datos MySQL mediante un entorno gráfico desde un navegador web. Esta herramienta facilita la gestión de la base de datos pues permite interactuar con ella sin mucha complejidad, aunque también permite gestionarse mediante consultas de lenguaje SQL y línea de comandos.

2.5 WEB3.JS

Como se ha explicado en los puntos anteriores, se ha visto que para programar el *back-end*, la lógica de la aplicación web, se usará Solidity que permitirá crear los Smart Contracts necesarios para que la aplicación funcione correctamente una vez desplegada sobre la red de blockchain. Por otro lado, se ha explicado también que los lenguajes HTML, CSS y JavaScript se utilizarán para desarrollar el *front-end*, el cual se ejecutará directamente sobre las máquinas de los clientes y permitirá a estos interactuar mediante una interfaz con la aplicación.

Por último, se necesita una lógica que permita conectar el *back-end* con el *front-end*, es decir, necesitamos una lógica que permita a la interfaz de la aplicación comunicarse con la red de blockchain y poder así consultar añadir o modificar datos en la red de blockchain. La herramienta que permite esto es Web3.js.

Web3.js es una interfaz de programación de aplicaciones (API), que incluye una amplia colección de librerías, que provee de métodos, los cuales, permiten interactuar con los nodos Ethereum de una red de blockchain local o remota mediante protocolos HTTP, IPC o WebSockets. Se puede encontrar la documentación en [12].

2.6 OTRAS HERRAMIENTAS USADAS

Para realizar de este proyecto, se han usado además otras herramientas que han permitido facilitar el desarrollo de la aplicación web.

2.6.1 GANACHE

Ganache consiste en una aplicación que permite simular una red de blockchain Ethereum con diferentes nodos y cuentas. Eso permite probar las aplicaciones descentralizadas directamente sobre esta red simulada, sin necesidad de probarlo en una red verdadera con los riesgos que ello puede llevar, como la pérdida de criptomonedas en transacciones erróneas cuando la aplicación que se está desarrollando no ha terminado de depurarse correctamente.

En este caso, puesto que se ha realizado un proyecto el cual puede entrar en conflictos con la legislación vigente sobre sucesiones y herencias, la aplicación no se ha desplegado sobre una red verdadera y se ha trabajado sobre Ganache para verificar su correcto funcionamiento. Más información y documentación en [13]

2.6.2 REMIX IDE

Se trata de un entorno de desarrollo interactivo que permite escribir Smart Contracts, compilarlos y desplegarlos en un emulador basado en JavaScript para comprobar su

funcionamiento. También permite desplegar contratos en redes de blockchain o aplicaciones como ganache. Incluye multitud de funciones como las de cualquier IDE conocido.

Este IDE se ha usado para escribir los Smart Contract en Solidity, es decir, se ha usado para programar la lógica de *back-end* que funcionará sobre la red de blockchain. Su documentación [14]

2.6.3 METAMASK

MetaMask [15] se trata de un monedero de criptomonedas. Es una extensión de navegadores web que además de actuar como monedero permite a los navegadores web interactuar con la red de blockchain de Ethereum. También servirá como forma de autenticación para la aplicación de este proyecto, pues para interactuar con una aplicación descentralizada, debes tener una cuenta y, por lo tanto, estar identificado en esta extensión.

2.6.4 ATOM

Atom [16] es uno de los editores de texto para programadores más comunes entre los desarrolladores. Permite usar diferentes lenguajes e instalar paquetes que faciliten a los desarrolladores su trabajo. En este caso, se ha usado para programar todo el *front-end* de la aplicación.

2.6.5 GOOGLE CHROME

Google Chrome [17] es un navegador web desarrollado por Google que permite navegar por internet y consultar páginas web. En este caso se ha usado para abrir en él la aplicación web que se ha creado y poder interactuar con la aplicación en local o remoto.

2.6.6 MINIWEB SERVER

MiniWeb Server [18] consiste en un pequeño servidor HTTP escrito en lenguaje C, el cual consume muy pocos recursos. En él se puede probar las páginas o aplicaciones web y conectarse a ellas de forma local o remota a través del puerto que abre el proceso en el dispositivo ejecutado.

2.6.7 WAMPSEVER

WampServer [19] se trata de un entorno de desarrollo para Windows que incluye multitud de herramientas para el desarrollo web. Algunas de las herramientas que se incluyen es el servidor Apache [20] que se trata de un servidor HTTP donde se pueden alojar las páginas web desarrolladas. Otras herramientas que incluye, mencionadas a lo largo de este apartado son MySQL, phpMyAdmin, PHP y demás. La ventaja de este entorno es que incluye todas las herramientas necesarias para el desarrollo web y pueden administrarse desde una misma aplicación permitiendo una amplia variedad de configuraciones y sin necesidad de estar instalándolas por separado realizando conexiones entre los distintos servicios.

Capítulo 3. ESTADO DE LA CUESTIÓN

En este capítulo se detalla el estado actual del caso de uso que se va a abordar en este Trabajo Fin de grado y el estado de la tecnología principal que se va a usar para su desarrollo, Blockchain.

3.1 BLOCKCHAIN

Como se ha mencionado en el apartado anterior, Blockchain comenzó a funcionar con el proyecto Bitcoin. Esto dio lugar durante los siguientes años al desarrollo de esta tecnología y mejoras de su funcionamiento además de su aplicación en el campo de la criptomoneda.

3.1.1 FUNCIONAMIENTO DE BLOCKCHAIN

La red de Blockchain se ideó y comenzó a usar para dar soporte al proyecto Bitcoin, y su funcionamiento estaba por lo tanto orientado a explicar cómo se realizaban transacciones bancarias.

Cuando se desea hacer una transacción bancaria entre dos personas, A y B, antes de la aparición de Blockchain, los bancos eran los encargados de realizar la transacción entre las cuentas de dichas personas. Tanto en el pasado como en la actualidad se dirigían a la cuenta de A y le restaban la cantidad que se transfería a B y en ocasiones una pequeña comisión, luego se dirigían a la cuenta de B y le sumaban la cantidad que se deseaba traspasar y la pequeña comisión la sumaban a la cuenta del banco. Antes todo esto se hacía en un libro mayor de cuentas apuntando los números y la transacción en él, actualmente se hace mediante programas informáticos y bases de datos, pero el funcionamiento es exactamente el mismo.

Como se ha visto, la figura del banco es la encargada de dar fe de que se realiza la transacción y la que manipula los libros mayores para evitar, en la medida de lo posible, que se manipulen las cuentas a traición. Aun así, este sistema es corruptible ya que está abierto a

fallos humanos o modificaciones malintencionadas, no solo en los bancos, sino también en las empresas cuando el intermediario es el departamento de contabilidad o un tesorero en vez del banco. El problema radica en que la confianza de que se realice la transacción se le otorga a una única entidad, persona o grupo de personas.

Blockchain permite que esta confianza quede depositada en toda una red descentralizada, de tal forma que cada nodo es anónimo y al trabajar con algoritmos asimétricos se garantiza la seguridad.

El ejemplo anteriormente explicado aplicado en Blockchain consistiría en que cuando A desea hacer un traspaso de dinero a B, todos los nodos reciben la orden de dicha transacción junto con otras muchas transacciones, las agrupa en un bloque y genera un hash de dicho bloque resolviendo un problema matemático. El primer nodo en resolver el problema matemático es recompensado con una pequeña comisión y comparte con el resto de los nodos la solución, los cuales comprueban que es correcta y si están de acuerdo el bloque queda firmado por el nodo que solucionó el acertijo. El bloque que queda numerado contiene también el número del bloque siguiente y anterior por lo que están encadenados. Por lo tanto, si algún nodo intentase modificar la transición, debido a las características del algoritmo hash, al ser distinta la cadena generada durante el minado del bloque a la del resto de nodos, dicho bloque modificado a traición sería ignorado por la red ya que su hash no sería igual que el generado por la mayoría de ellos nodos (51%).

El proceso por el cual los nodos solventan el problema matemático para obtener el hash del bloque es denominado comúnmente como “minado” y el resultado de minar varios bloques, identificados cada uno por su hash, es una cadena de bloques “Blockchain”.

A continuación, en la *Ilustración 1* se muestra un esquema del funcionamiento de la tecnología de Blockchain desde un punto de vista de alto nivel.

CÓMO FUNCIONA EL BLOCKCHAIN

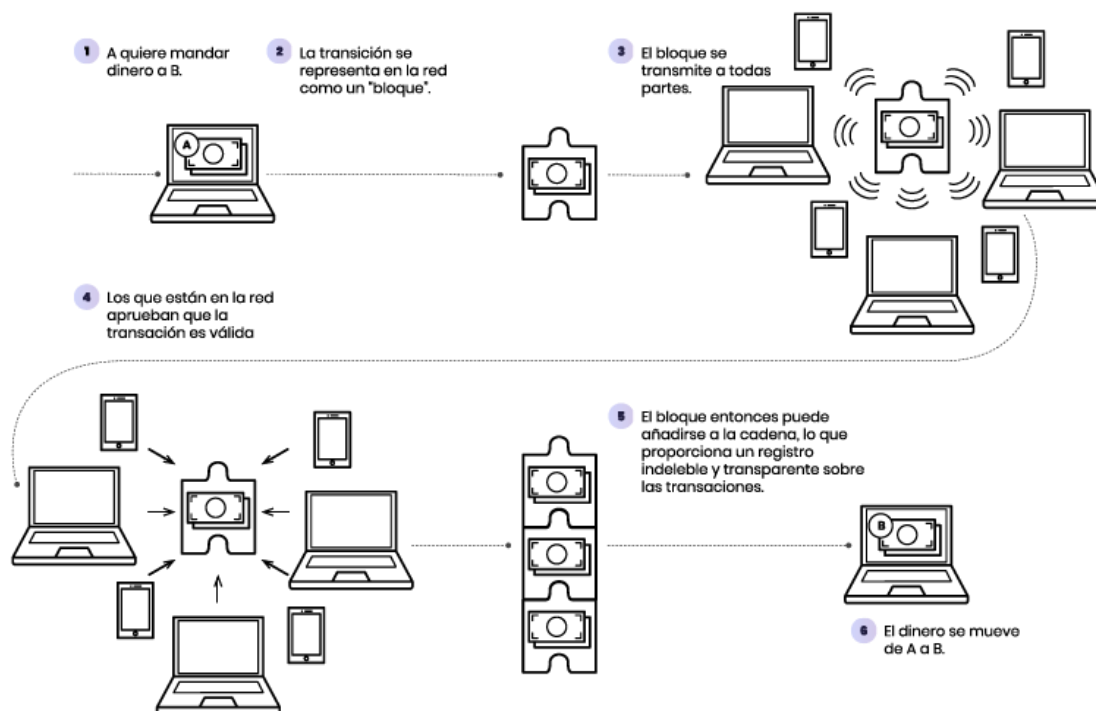


Ilustración 1. Funcionamiento de Blockchain

Como se ha visto hasta ahora, el trabajo que desempeñaba el banco y la confiabilidad que se depositaba en este puede ser sustituida por una red descentralizada con un sistema de Blockchain, pero se necesita una forma para que los nodos puedan ponerse de acuerdo entre ellos, en quien ha solucionado el problema matemático antes (minando), o cuando un bloque es válido y cuando no. Para esto existen los algoritmos de consenso.

3.1.2 ALGORITMOS DE CONSENSO

Los algoritmos de consenso son mecanismos que permiten a los nodos de las redes de blockchain acordar el estado correcto de un registro cuando se ha realizado una o varias transacciones y minado de un bloque. Véase [21]

3.1.2.1 Proof of Work (PoW)

El primer proyecto Blockchain, Bitcoin, se implantó usando el algoritmo ***“Proof of Work”***. Este algoritmo requiere que los nodos realicen un trabajo, en este caso resolviendo un problema matemático complejo mediante prueba y error, para el que se requiere alta capacidad computacional. Resolver el problema es complicado y requiere de esta capacidad mencionada, pero en cambio comprobar el resultado es muy fácil ya que simplemente consiste en generar un hash con unos parámetros determinados, estos parámetros establecen los requisitos para la complejidad del problema. Por lo tanto, cuando un nodo consigue resolver el acertijo matemático, comparte su solución y los parámetros usados con el resto de los nodos de la red que comprueban que cumplen los requisitos del acertijo. Si como mínimo el 51% de la red da por buena la solución, se determina que se ha resuelto el problema matemático, y el bloque queda minado y asegurado, por lo que se comparte la información con todos los nodos de la red para que, si en cualquier momento un cliente desea consultar la información de una transacción perteneciente al bloque minado, lo podrá hacer directamente en cualquiera de los nodos de la red y no solo en el que resolvió el acertijo.

PoW es un protocolo muy ventajoso [22] en el campo que ocupaba Bitcoin ya que:

- Resiste a ataques de Denegación de servicios.
- Tiene una fácil implementación y adaptabilidad a las diferentes necesidades de hardware y diferentes avances tecnológicos (a medida que avanza la tecnología y los equipos hardware, el algoritmo se puede adaptar).

Pero no siempre interesa utilizar este algoritmo para todas las redes Blockchain ya que presenta diferentes desventajas [23] debido a:

- Altos costes que tienen los equipos hardware a medida que pasa el tiempo, ya que el problema o acertijo matemático se complica y se requiere de mayor capacidad computacional y energía eléctrica.

- Inutilidad de cálculos realizados, ya que el algoritmo realiza múltiples cálculos inútiles hasta que encuentra la solución del acertijo matemático (todos los resultados calculados del problema matemático que se desechan).
- Finalmente, por la regla del 51% de ataque. Como se ha visto anteriormente, para que un bloque se haya minado con satisfacción, al menos el 51% de los nodos de la red tienen que confirmar que la solución obtenida es válida. Es decir, al menos el 51% de la red debe de estar de acuerdo en la solución, por lo tanto, si nos encontramos en una red en la que el 51% o más de los nodos están bajo el control de una misma entidad o dueño, este podría tener el control de toda la red y no serviría de nada el sistema Blockchain. Por lo tanto, este algoritmo es válido para redes públicas, con grandes números de nodos y clientes como Bitcoin o Ethereum donde es muy complicado que una sola persona o entidad disponga del 51% de la red.

3.1.2.2 Otros algoritmos de consenso

Como se ha visto en el algoritmo *Proof of Work*, no siempre interesaría usar este algoritmo de consenso. Debido a esto, según la finalidad de la red Blockchain y de los requisitos, como una red privada o pública, existen otros tipos de algoritmos de consenso (Véase [21]):

- Redes privadas: Cuando se tiene una red privada (por ejemplo, para una empresa), el algoritmo más usado es ***Proof of Authority***. Este algoritmo basa su funcionamiento en que al consistir en una red privada los nodos no actúan de forma anónima y muestran su identidad real en la red, proponiendo su reputación como una garantía de transparencia firmando transacciones con sus certificados digitales, por lo que, se garantiza la transparencia en la firma de bloques, ya que la responsabilidad recae directamente en el nodo que realiza la operación. En este algoritmo, no participan todos los nodos para firmar un bloque, sino que, se selecciona de forma aleatoria unos nodos que serán los validadores de tal forma que, en una consecución de bloques, un mismo validador solo podrá participar en la firma de un bloque como máximo. Este algoritmo también garantiza confiabilidad ya que lo que cada nodo pone en juego es su reputación en la red.

- Redes públicas: Cuando nos encontramos en redes públicas existen otros dos algoritmos muy conocidos además del *Proof of Work*:
 - ***Proof of Stake (PoS)***: los nodos que se transforman en validadores de bloques dependen de la inversión que tienen en dicha red. De esta forma, su fiabilidad depende de la cantidad invertida en dicha red puesto que a mayor inversión más pérdidas puede tener el nodo.
 - ***Proof of Elapsed Time (PoET)***: es usado no solo en redes públicas, sino que también se puede usar en redes privadas. Este algoritmo consiste en nombrar como validador al primer nodo que complete el acertijo matemático de un bloque transcurrido un tiempo aleatorio.

Después del proyecto Bitcoin muchos proyectos han usado la tecnología Blockchain para llegar a término con sus trabajos, entre ellos están otras criptomonedas como Ripple y Litecoin o proyectos que van más allá como Hyperledge o Ethereum, plataforma de código abierto que permite el desarrollo de aplicaciones descentralizadas (Dapps) y Smart Contracts.

3.1.3 ESTADO ACTUAL DE BLOCKCHAIN Y CRIPTOMONEDAS

Como se ha visto en 2.1 *Blockchain*, Blockchain comenzó a usarse en el proyecto Bitcoin dando lugar a la aparición de las criptomonedas.

Las criptomonedas consisten en un tipo de divisa “*peer to peer*” (P2P) digital. Esta, al aprovecharse de las ventajas de Blockchain, se convierte en una divisa segura que no requiere de una autoridad central de control como el resto de las divisas conocidas, ya que las criptomonedas se manejan en una red descentralizada en la que no hay un servidor central como intermediario. La primera criptomoneda fue el Bitcoin (BTC) aunque con el paso del tiempo han aparecido más criptomonedas como Ethereum (ETH) y Litecoin (LTC) entre otras.

Con la irrupción de las criptomonedas han aparecido dos nuevos modelos de inversión. Por un lado, la compra-venta de activos asociados a las criptodivisas, de la misma forma que ocurre con las distintas divisas que encontramos en el mercado con la diferencia de que las

criptodivisas tienen tendencia a una mayor fluctuación y esto implica un riesgo más alto que no está totalmente regulado ni controlado por un mercado central.

Por otro lado, existe la posibilidad de invertir en la infraestructura que se utiliza para el minado de las criptomonedas, de tal forma que se puede invertir en hardware para el minado o asociarse en un pool de minería. Como ya se vio en *Descripción de las Tecnologías*, en Blockchain, se produce un proceso llamado minado en el que se calcula un problema o acertijo matemático mediante prueba y error y el nodo que primero lo resuelve obtiene una recompensa en BTC o en la criptomoneda que se esté operando; los nodos compiten entre ellos para firmar un bloque de la blockchain y el nodo que mayor capacidad de cómputo tenga es el que más posibilidades tiene de resolver el acertijo matemático en el menor tiempo. Cuando apareció el Bitcoin por primera vez era muy sencillo resolver el problema matemático pero debido a que está calculado el número máximo de bitcoins que habrá en total circulando en 21 millones BTC, y estos se van poniendo en circulación lentamente, el problema matemático se ha ido complicando para dosificar la expedición de BTC y no llegar rápidamente a los 21 millones BTC. Además, cada cierto tiempo se reduce a la mitad la recompensa obtenida por minar un bloque, proceso conocido como “*halving*”.

Por tanto, al comienzo cualquier persona podía minar bitcoins con facilidad desde un ordenador, pero en la actualidad es muy complicado haciendo uso de un ordenador convencional conseguir minar un bloque y así obtener una recompensa. Es por esto por lo que la gente invierte en hardware (GPUs, que son las que mejor realizan este cálculo) que permita aumentar la capacidad de cómputo y así conseguir minar bloques.

A continuación, en Ilustración 2 se presenta un cuadro donde se puede ver la evolución de la recompensa dependiendo del número de bitcoins que hay en circulación. Actualmente nos encontramos en la 4ª era, ya que el pasado mayo de 2020 se produjo el último *halving* reduciéndose la recompensa de 12.5 BTC a 6.25 BTC con un total de 18,375,000 Bitcoins minados.

Bloque	Era recompensa	BTC/bloque	BTC Inicio	BTC añadido	BTC Finales	Incremento BTC	% BTC del límite en circulación
0	1	50,00000000	0,00000000	10.500.000,000000	10.500.000,000000	Infinito	50,00000006%
210000	2	25,00000000	10.500.000,000000	5.250.000,000000	15.750.000,000000	50,00000000%	75,00000008%
420000	3	12,50000000	15.750.000,000000	2.625.000,000000	18.375.000,000000	16,66666667%	87,50000010%
630000	4	6,25000000	18.375.000,000000	1.312.500,000000	19.687.500,000000	71,42857140%	93,75000010%
840000	5	3,12500000	19.687.500,000000	656.250,000000	20.343.750,000000	33,33333330%	96,87500011%
1050000	6	1,56250000	20.343.750,000000	328.125,000000	20.671.875,000000	16,12903230%	98,43750011%
1260000	7	0,78125000	20.671.875,000000	164.062,500000	20.835.937,500000	0,79365079%	99,21875011%
1470000	8	0,39062500	20.835.937,500000	82.031,250000	20.917.968,750000	0,39370079%	99,60937511%
1680000	9	0,19531250	20.917.968,750000	41.015,625000	20.958.984,375000	0,19607843%	99,80468761%
1890000	10	0,09765625	20.958.984,375000	20.507,812500	20.979.492,187500	0,09784736%	99,90234386%
2100000	11	0,04882812	20.979.492,187500	10.253,905200	20.989.746,092700	0,04887585%	99,95117198%
2310000	12	0,02441406	20.989.746,092700	5.126,952600	20.994.873,045300	0,02442599%	99,97558604%
2520000	13	0,01220703	20.994.873,045300	2.563,476300	20.997.436,521600	0,01221001%	99,98779307%
2730000	14	0,00610351	20.997.436,521600	1.281,737100	20.998.718,258700	0,00610426%	99,99389658%
2940000	15	0,00305175	20.998.718,258700	640,867500	20.999.359,126200	0,00305194%	99,99694833%
3150000	16	0,00152587	20.999.359,126200	320,432700	20.999.679,558900	0,00152592%	99,99847420%
3360000	17	0,00076293	20.999.679,558900	160,215300	20.999.839,774200	0,00076294%	99,99923713%
3570000	18	0,00038146	20.999.839,774200	80,106600	20.999.919,880800	0,00038146%	99,99961859%
3780000	19	0,00019073	20.999.919,880800	40,053300	20.999.959,934100	0,00019073%	99,99980932%
3990000	20	0,00009536	20.999.959,934100	20,025600	20.999.979,959700	0,00009536%	99,99990468%
4200000	21	0,00004768	20.999.979,959700	10,012800	20.999.989,972500	0,00004768%	99,99995236%
4410000	22	0,00002384	20.999.989,972500	5,006400	20.999.994,978900	0,00002384%	99,99997620%
4620000	23	0,00001192	20.999.994,978900	2,503200	20.999.997,482100	0,00001192%	99,99998812%
4830000	24	0,00000596	20.999.997,482100	1,251600	20.999.998,733700	0,00000596%	99,99999408%
5040000	25	0,00000298	20.999.998,733700	0,625800	20.999.999,359500	0,00000298%	99,99999706%
5250000	26	0,00000149	20.999.999,359500	0,312900	20.999.999,672400	0,00000149%	99,99999855%
5460000	27	0,00000074	20.999.999,672400	0,155400	20.999.999,827800	0,00000074%	99,99999929%
5670000	28	0,00000037	20.999.999,827800	0,077700	20.999.999,905500	0,00000037%	99,99999966%
5880000	29	0,00000018	20.999.999,905500	0,037800	20.999.999,943300	0,00000018%	99,99999984%
6090000	30	0,00000009	20.999.999,943300	0,018900	20.999.999,962200	0,00000009%	99,99999993%
6300000	31	0,00000004	20.999.999,962200	0,008400	20.999.999,970600	0,00000004%	99,99999997%
6510000	32	0,00000002	20.999.999,970600	0,004200	20.999.999,974800	0,00000002%	99,99999999%
6720000	33	0,00000001	20.999.999,974800	0,002100	20.999.999,976900	0,00000001%	100,00000000%
6930000	34	0,00000000	20.999.999,976900	0,000000	20.999.999,976900	0,00000000%	100,00000000%

Ilustración 2. Evolución de la expedición de BTC respecto al número de bloques minados y recompensas por bloque minado

También cabe la posibilidad de asociarse en un pool de minería, el cual consiste en un grupo de usuarios que pone al servicio del grupo su capacidad de cómputo junto con el del resto de socios y si el grupo consigue minar en conjunto un bloque, la recompensa se divide de forma proporcional a la capacidad de cómputo de los miembros asociados.

Con el paso del tiempo, las criptomonedas, se han convertido en algo más que un activo para inversores. A día de hoy, el Bitcoin (BTC) se está extendiendo como método de pago entre la población y ya hay muchas tiendas donde los clientes pueden realizar pagos con esta criptomoneda.

Por otro lado, criptomonedas como Ether (ETH) y la red Ethereum han dado lugar a mayor evolución y desarrollo puesto que permite crear aplicaciones descentralizadas y esto abre las puertas a nuevos proyectos apoyados sobre esta red y la tecnología de Blockchain.

3.1.4 APLICACIONES DESCENTRALIZADAS Y PROYECTOS APOYADOS SOBRE ETHEREUM

Los proyectos que se desarrollan en Ethereum se caracterizan porque buscan la confiabilidad y seguridad que provee la red de Blockchain. Existen múltiples proyectos en la actualidad dedicados a diferentes campos.

En el campo de la computación, existe el proyecto Golem [24], que a partir de la red de blockchain y los Smart Contracts, permite usar la potencia de cómputo de los dispositivos conectados a una red descentralizada, con el fin de lograr la capacidad de un super ordenador capaz de suministrar recursos para desarrolladores y usuarios que requieren de altas capacidades computacionales para realizar tareas como la renderización multimedia.

También existen proyectos más allá de la ingeniería, en el campo de los seguros, una empresa llamada Signaturit [25] dedicada a proveer servicios que garanticen la seguridad jurídica en transacciones digitales, ha comenzado un proyecto junto con DAS Seguros [26] con la finalidad de automatizar los pagos de pólizas de seguros mediante la tecnología Blockchain y Smart Contract, y además permitir una trazabilidad completa desde que se contratan sus servicios.

En campo jurídico existe un proyecto muy interesante, más orientado al campo jurídico y relacionado con este trabajo fin de grado. Se da en Chile y allí la empresa Madesal, una empresa inmobiliaria del país, y la startup Plexus, la cual implementa soluciones de contabilidad distribuida, juntas buscan crear un registro de bienes raíces (inmuebles). Esta solución es interesante pues además de facilitar el proceso de compra y automatizar el proceso de pago, crea un registro sobre la red de blockchain que permitiría interactuar con la aplicación que se busca crear en este trabajo fin de grado sobre herencias y sucesiones. Más información sobre el proyecto en [27].

3.2 ESTADO DE LA CUESTIÓN DEL PROCESO DE TESTAMENTARÍA Y HERENCIA.

Como ya se ha indicado en la introducción en *Capítulo 1.*, este Trabajo Fin de Grado busca contribuir en la mejora del proceso de elaboración de testamentos y proceso de herencia haciendo uso de nuevas tecnologías como Blockchain y Smart Contract.

En la actualidad, el proceso de elaboración del testamento comienza acudiendo a un notario, el cual se encarga de elaborar un escrito conocido como testamento³ (Véase en [28]) que refleja las últimas voluntades de un cliente en presencia de dos testigos. Un mismo cliente puede repetir este proceso tantas veces como quiera, es decir, puede realizar todos los testamentos que desee de tal forma que en el momento de la defunción el último testamento será el que tiene validez.

Cuando una persona fenece, comienza el proceso de herencia. El proceso se inicia a partir de un certificado médico de defunción en el que un médico o forense expresa en términos médicos el fallecimiento. Es decir, es un informe médico que indica el suceso de la defunción. A partir de este documento, se elabora el Certificado de Defunción del Registro Civil, documento legal con validez jurídica que hace constar la defunción de la persona junto a la fecha, lugar, médico que corrobora el suceso y demás datos.

Después de la defunción de una persona, quedan bloqueados todos sus bienes a la espera de la resolución del destino de estos para evitar su uso fraudulento.

Pasados quince días hábiles desde fallecimiento, se solicita en el Ministerio de Justicia el Certificado de Últimas Voluntades a partir del Certificado de Defunción. En el Certificado de Últimas Voluntades figuran los datos de la persona en cuestión como la fecha de

³ Testamento: En el ámbito legal, el testamento es “El acto por el cual una persona dispone para después de su muerte de todos sus bienes o parte de ellos” (CC 667) Ver [28]. El testamento es un acto jurídico con los siguientes caracteres: a) Mortis causa y unilateral, b) Otorgado por una sola persona, c) Personalísimo, d) Libre, e) Formal y solemne, f) Esencialmente revocable. Véase [31]

nacimiento, fecha de defunción y, además, todos los testamentos que la persona ha otorgado, o no, en vida junto con el número de protocolo, notario, fecha de creación y otros datos de cada testamento.

Con el Certificado de Últimas Voluntades se acude a un notario para que este solicite una copia del testamento al Colegio de Notarios pues ellos tienen centralizada toda esta información.

El notario es una figura imprescindible en todo el proceso ya que, aunque los familiares dispongan de una copia del testamento, el notario es el encargado de identificar a partir del testamento toda la masa hereditaria (escrituras de la propiedad, saldos de los bancos a fecha de fallecimiento, etc.), a todos los posibles herederos y supervisar el traspaso de bienes sin ninguna controversia.

Una vez que el notario tiene toda esta información lista, reúne a los herederos para la lectura del testamento de forma presencial e informar a cada uno de la situación y los bienes que les corresponden. Los herederos, una vez informados en la reunión, deben aceptar o renunciar a la herencia con todo lo que conlleva como deudas, bienes inmuebles y demás. También existe la opción de aceptar en beneficio, lo que significa que solo heredan el valor neto de los bienes, sin deudas.

Cabe la posibilidad de que la persona que fallece no haya escrito testamento (Intestado), por lo que los ascendientes, descendientes o colaterales podrían proceder mediante vía judicial por una demanda que daría lugar a trámite en juicio y a una investigación para recopilar la masa hereditaria y fallar a favor o en contra de los solicitantes.

Mas adelante, en el apartado 5.1, se realizará un análisis de este modelo con el fin de obtener las pautas necesarias para diseñar un nuevo modelo basado en las tecnologías Blockchain y Smart Contract.

3.3 PROYECTOS DE TESTAMENTARÍA Y HERENCIAS BASADOS EN BLOCKCHAIN

Actualmente existe una empresa en España que ha intentado abordar casuísticas similares a la presentada en este Trabajo Fin de Grado.

Existe un problema con los activos digitales de las personas cuando estas fallecen ya que durante su vida crean cuentas en redes sociales, contenido multimedia y demás que cuando se produce la defunción del propietario de dicho contenido, este continua en la red sin ningún dueño y sin control. Con el fin de atajar este problema, una empresa llamada Mi Legado Digital [29] permite elaborar testamentos digitales donde los clientes pueden traspasar estos activos a los herederos designados cuando fenecen. Esta misma empresa ofrece la posibilidad de crear un testamento “inteligente”, el cual incluye diferentes servicios como el testamento digital y un testamento online donde se pueden testar los bienes, objetos personales y otras propiedades que forman la masa hereditaria con el fin de que una vez que se hace dicho testamento se acuda al notario para que este lo valide. Esta empresa también hace uso de la tecnología Blockchain para el almacenado de esta información, pero sigue siendo necesario acudir a un intermediario o persona que valide el trámite, el notario, tanto cuando se está elaborando, como cuando se produce la defunción.

La diferencia con este Trabajo Fin de Grado es que uno de los objetivos es demostrar que existe la tecnología suficiente para evitar acudir a intermediarios que validen estas operaciones, aunque no se puede implantar debido a la legislación vigente si se puede demostrar que existe una alternativa más ágil, segura, transparente y automática que la tradicional.

Capítulo 4. DEFINICIÓN DEL TRABAJO

4.1 JUSTIFICACIÓN

En este trabajo fin de grado se va a desarrollar una aplicación web en la que los clientes podrán realizar sus testamentos que podrán ser ejecutados de forma automática cuando se produzca la defunción de estos, dando así lugar al reparto de los bienes inmuebles tal y como se había establecido en las últimas voluntades del difunto.

Como se ha visto en el apartado 3.2, el proceso de elaboración de testamentos y herencia es un proceso lleno de trámites y certificados los cuales si no tienes un mínimo conocimiento de ellos es complicado llegar hasta el final del proceso sin ayuda legal. Este proceso no solo es largo y complejo, además puede convertirse en un proceso muy costoso, no solo sentimentalmente, sino económicamente, impidiendo en muchas ocasiones que los herederos puedan afrontar los gastos. Esto es debido al número de trámites que hay que realizar, impuestos a pagar y el importante papel que desempeñan los notarios y figuras legales de por medio en los que se deposita plena confianza para que verifiquen y controlen que no se produce ningún fraude en el traspaso de bienes, como la manipulación del testamento para favorecer a determinados herederos, aumentar la masa hereditaria u otras irregularidades.

A la vista de esta situación, con el fin de facilitar todo el proceso de elaboración de testamento, así como el proceso de herencia, y con el fin de dotar a estos de transparencia y la confiabilidad requerida por dichos procesos tan delicados, se ha optado por implementar una aplicación web descentralizada soportada sobre la red de Blockchain y tecnología Smart Contract para garantizar que los testamentos sean incorruptibles y evitar que puedan ser manipulados a traición a favor de ningún heredero. Es decir, en esta aplicación descentralizada, la confianza depositada en la figura del notario y sus funciones, quedan sustituidas por las características intrínsecas de la tecnología Blockchain y Smart Contract.

En esta aplicación, todos los clientes podrán realizar sus propios testamentos, crear tanto como quieran y nombrar a los herederos de sus propiedades con el fin de que cuando se produzca la defunción del testador, los herederos puedan en la misma aplicación aceptar o rechazar la herencia y automáticamente se realice una reasignación de toda la masa hereditaria y traspaso de estos bienes.

Como consecuencia de este desarrollo, no solo desaparecería la figura del notario, también se verían reducidos los costes y trámites que los usuarios deber realizar a la hora de escribir un testamento y en el proceso de herencia. También permite tener pleno control sobre el proceso al usuario, sin que intervengan terceras personas en él.

4.2 OBJETIVOS

Como ya se ha indicado a lo largo de este documento, el fin de este Trabajo Fin de Grado es el desarrollo de una plataforma que permita disminuir la capacidad del proceso de elaboración del testamento y herencia. Para ellos se han marcado los siguientes objetivos:

- Desarrollo de una aplicación web descentralizada en la que el usuario o testador pueda confeccionar tantos testamentos como deseé, de tal forma que en el momento de la defunción tenga validez el último de ellos.
- Integración de la tecnología Blockchain y Smart Contract con el fin de otorgar la confiabilidad y seguridad que la aplicación requiere para garantizar que los testamentos sean transparentes e incorruptibles, evitando que puedan ser modificados a traición y puedan ser ejecutados de forma automática como si de contratos inteligentes se tratasen para poder realizar el reparto de bienes de forma automática sin necesidad de figuras intermediarias.
- Simulación de una red descentralizada para validar el correcto funcionamiento de la aplicación y de todo el proceso de herencia descrito.

4.3 METODOLOGÍA

Para llevar a cabo la realización de este proyecto, se ha hecho uso de una metodología *Agile*. Esta metodología de trabajo permite la entrega temprana y continua de software, lo que ha permitido a medida que se iba avanzando poder realizar demostraciones del funcionamiento de la aplicación a los directores de proyecto, a medida que se iba desarrollando, en periodos de tiempo cortos.

Para planificar las tareas y entregas se ha usado un diagrama de Gantt que ha ido cambiando a medida que ha transcurrido el tiempo de duración del proyecto. En Ilustración 3 podemos ver dicho diagrama de Gantt con la planificación del proyecto llevado durante el curso 2019/2020.

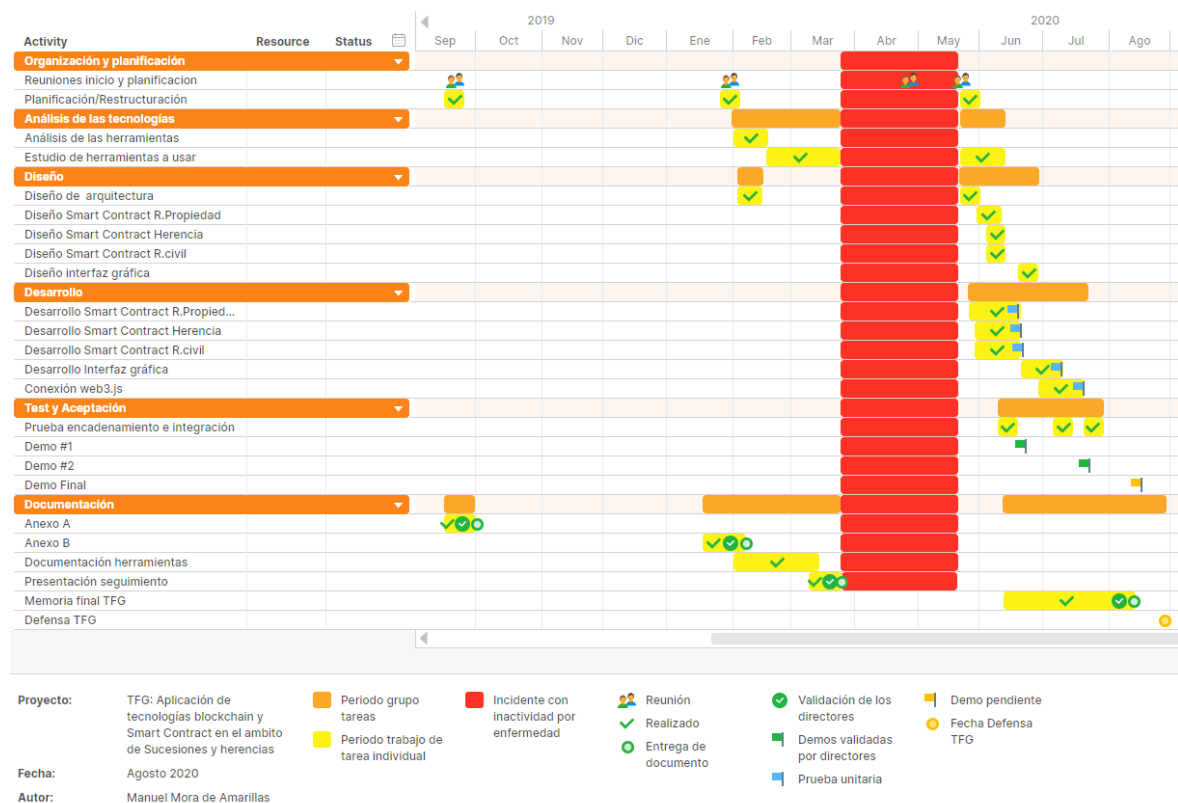


Ilustración 3. Diagrama de Gantt con las tareas del proyecto

Además, siguiendo con la línea del método *Agile*, se ha realizado un *backlog* con todas las funcionalidades que debían tener los Smart Contracts desarrollados (que veremos más

adelante en detalle). Esto ha permitido tener una lista continuamente actualizada con todas las funcionalidades que se deseaban implantar en la aplicación web. Para ello se ha usado un *panel Kanban* en la aplicación Trello, ver Ilustración 4, en el que se puede visualizar el estado de todas las funcionalidades si están en proceso de desarrollo, pendientes o terminadas. El *panel Kanban* es muy útil para trabajar en grupos de desarrolladores de tal forma que todos los ingenieros o participantes son conscientes en todo momento del estado del desarrollo, aunque en este caso, siendo un solo miembro, también ha sido útil para organizar el trabajo.

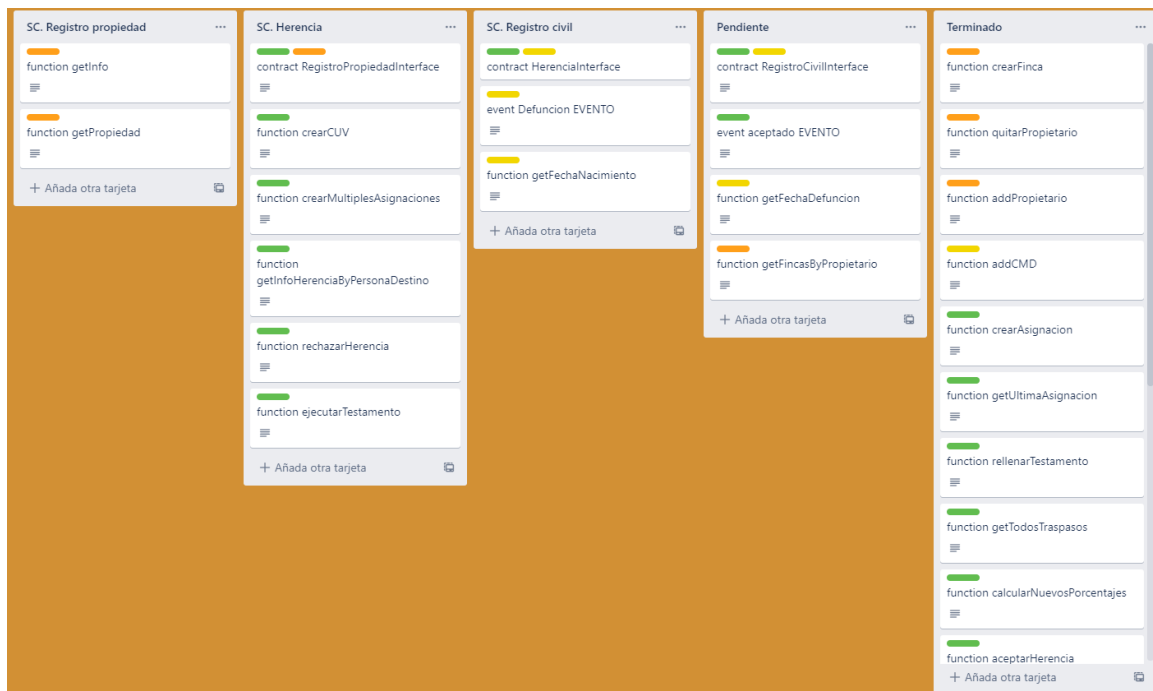


Ilustración 4. Panel Kanban del backlog del proyecto

4.4 ESTIMACIÓN ECONÓMICA

En este apartado, se presenta una estimación económica del coste del desarrollo de este proyecto en función de los recursos materiales y humanos.

4.4.1 RECURSOS MATERIALES

En cuanto a los recursos materiales usados para el desarrollo del trabajo fin de grado se ha usado un ordenador portátil, cuyas características pueden verse en Tabla 1, y un monitor auxiliar cuyas características pueden verse en Tabla 2.

Ordenador portátil MSI PS42 8RB	
CPU	8th Gen. Intel® Core™ i7 U-Processor
Sistema operativo	Windows 10 Home
Pantalla	14.0" FHD (1920x1080), IPS-Level
Tarjeta gráfica	Geforce® MX150 with 2GB GDDR5
Memoria RAM	DDR4-2400Hz 16GB
Disco Duro	1x M.2 SSD 500 GB
Precio	1.199,00 €

Tabla 1. Especificaciones de ordenador portátil

Monitor HP E233	
Resolución bruta	FHD (1920 x 1080 a 60 Hz)
Tipo de pantalla	IPS con retroiluminación LED
Proporción	16:9
Tipo de entrada de video	1 VGA, 1 HDMI, 1 DisplayPort
Memoria RAM	DDR4-2400Hz 16GB
Precio	199,00 €

Tabla 2. Especificaciones monitor auxiliar

Actualmente un ordenador portátil tiene una vida útil fiscal de cuatro años (35.040 horas), la vida útil fiscal de un monitor es de 60.000 horas activo. Además, ambos dispositivos se han usado para otras tareas por lo que su uso no ha sido exclusivamente para este trabajo. El tiempo que se ha usado ambos dispositivos está detallado en Tabla 3 con un total de 905 horas. Por lo que en la Ecuación 1 y Ecuación 2 podemos ver el precio de ambos recursos

materiales por horas y en la *Ecuación 3* y *Ecuación 4* el precio total de cada recurso en este proyecto.

Actividad	Horas
Organización, planificación y reuniones	20 horas
Análisis y estudio de tecnologías	135 horas
Diseño	400 horas
Desarrollo	50 horas
Pruebas	300
Documentación del proyecto	
TOTAL	905 horas

Tabla 3. Horas de trabajo

$$\text{Coste por hora (Ordenador Portatil)} = \frac{1.199,00 \text{ €}}{35.040 \text{ horas}} = 0,0342 \text{ €/hora}$$

Ecuación 1. Coste por horas del ordenador portátil

$$\text{Coste por hora (Monitor)} = \frac{199,00 \text{ €}}{60.000 \text{ horas}} = 0,0033 \text{ €/hora}$$

Ecuación 2. Coste por horas del monitor auxiliar

$$\text{Coste total (Ordenador portatil)} = \frac{905}{35.040} \times 1.199,00\text{€} = 30,96\text{€}$$

Ecuación 3. Coste total del ordenador portátil durante el proyecto

$$\text{Coste total (Monitor)} = \frac{905}{60.000} \times 199,00\text{€} = 3,00\text{€}$$

Ecuación 4. Coste total del monitor auxiliar durante el proyecto

En cuanto al software utilizando, todos los programas utilizados son de libre distribución por lo que no requiere de coste adicional. De esta forma, el precio total de los recursos materiales quedaría como sigue en *Tabla 4*.

Concepto	Coste (€/hora)	Tiempo de uso (horas)	Coste total de recurso
Ordenador portátil “MSI PRESTIGE PS42 8RB”	0,0342 €/hora	905 horas	30,96 €
Monitor “HP E233 23 pulgadas”	0,0033 €/hora	905 horas	3,00 €
TOTAL			33,96 €

Tabla 4. Costes de recursos materiales

4.4.2 RECURSOS HUMANOS

En cuanto a los recursos humanos utilizados para llevar a cabo este proyecto se ha tratado del trabajo realizado por un desarrollador y la asesoría legal de un abogado sobre derecho de sucesiones y herencias.

Actualmente, los honorarios del trabajo desempeñado por un desarrollador de media en España son de 45 €/hora. Por otro lado, el coste por hora de un abogado según las normas de criterios de honorarios de abogados es de 80 €/hora de media por prestar servicios de consultorías.

El tiempo de trabajo del desarrollador es el mismo tiempo calculado en *Tabla 3. Horas de trabajo* del apartado anterior, mientras que el abogado a prestado sus servicios de consultoría durante cinco horas. De esta forma, el precio total de los recursos humanos puede verse detallado en *Tabla 5*

Concepto	Coste (€/hora)	Tiempo trabajado (horas)	Coste total de recurso (€)
Desarrollador	45 €/hora	905 horas Tabla 3. Horas de trabajo	40.725,00 €
Consultoría legal	80 €/hora	5 horas	400,00 €
TOTAL			41.125 €

Tabla 5. Costes de recursos humanos

4.4.3 PRESUPUESTO TOTAL

A la vista del punto 4.4.1 y 4.4.2 y de acuerdo a los valores obtenidos, el presupuesto total del proyecto se detalla en *Tabla 6*, con un coste total de 41.158,96 € (Cuarenta y un mil ciento cincuenta y ocho euros con 96 céntimos).

Concepto	Detalle	Uds (horas)	Precio Ud (€/hora)	Precio (€)	Total (€)
Recursos materiales	Ordenador portátil	905 horas	0,0342 €/hora	30,96 €	
	Monitor	905 horas	0,0033 €/hora	3,00 €	
					33,96 €
Recursos humanos	Desarrollador	905 horas	45 €/hora	40.725,00 €	
	Abogado consultor	5 horas	80 €/hora	400,00 €	
					41.125,00 €
TOTAL				41.158,96 €	

Tabla 6. Coste total del proyecto

Capítulo 5. MODELO DESARROLLADO

En este capítulo se va a exponer el modelo desarrollado en este trabajo fin de grado que consiste en el caso de uso de la aplicación de las tecnologías de Blockchain y Smart Contracts en el ámbito legal de herencias y sucesiones, con el fin de demostrar que actualmente existe la tecnología suficiente para realizar estos procesos con total transparencia y sin riesgo de fraude o manipulación mal intencionada del testamento o herencia de una persona.

En primer lugar, se va a realizar un análisis del modelo actual y las pautas que siguen tanto el proceso de elaboración de un testamento, como el proceso de herencia. Esto permitirá tener consciencia de las necesidades y requisitos que debe abarcar el modelo para posteriormente plantear un diseño capaz de obtener los mismos resultados que el modelo actual.

5.1 ANÁLISIS DEL MODELO

Tanto para el análisis del modelo como para el desarrollo vamos a diferenciar en este sistema dos procesos distintos, por un lado, el proceso de elaboración de un testamento, y por otro el proceso de herencia.

En el apartado 4.1 ya se explicó en que consiste actualmente ambos procesos para tener un contexto de la necesidad de este proyecto, pero es necesario realizar un análisis de estos para poder extraer los pasos clave necesarios para el modelo propuesto a desarrollar.

5.1.1 ANÁLISIS DEL PROCESO DE ELABORACIÓN DE TESTAMENTOS

El proceso de elaboración del testamento abarca desde que un cliente muestra intención de expresar de forma voluntaria una declaración a través de un acto jurídico en el que dispone para después de su muerte de todos sus bienes o parte de ellos (CC 667), ver [28].

Si un cliente cambia de opinión y desea cambiar el testamento, no puede, lo que debe hacer es escribir uno nuevo. Por ello, un cliente puede elaborar tantos testamentos como desee pues a lo largo de su vida puede cambiar sus intenciones y últimas voluntades, pero cuando este fenezca, aunque todos los testamentos quedan registrados, solo tendrá validez el último de ellos.

Los pasos de los que consta la elaboración de un testamento se pueden dividir en tres:

1. **Acudir a la notaría:** Los clientes acuden con la documentación necesaria requerida por la notaría como las escrituras de las propiedades y documentos de identificación entre otros, necesarios para la redacción del testamento.
2. **Escritura del testamento:** Los oficiales y trabajadores de la notaría redactan el testamento a partir de la documentación proporcionada por los clientes y de sus últimas voluntades.
3. **Firma y registro del testamento:** Se acude a una cita con el notario y en su presencia, los clientes firman el testamento y posteriormente el notario se encarga de registrarlo.

A continuación, en *Ilustración 5* se muestra un diagrama que refleja los pasos principales para llevar a cabo el proceso de elaboración de testamento.

Elaboración Testamento

1

Acudir a la Notaría

Se acude con documentación necesaria (escrituras) para la redacción del testamento



2

Se escribe el Testamento

Escritura del testamento por parte de los Oficiales y trabajadores de la notaría



3

Firma y registro del Testamento



Ilustración 5. Proceso de elaboración de Testamento con modelo tradicional

A partir de estos tres pasos, se busca una adaptación para que la aplicación a desarrollar pueda realizar el mismo proceso.

En primer lugar, no será necesario presentar documentación ni acudir a la notaría, la aplicación descentralizada buscará directamente en el Registro de la Propiedad los bienes inmuebles del cliente.

El cliente tampoco tendrá que esperar a que se redacte un documento con sus voluntades, directamente podrá expresar sus deseos en la aplicación desarrollada asignando las propiedades de las que disponga a los futuros herederos. En este trabajo solo se van a tener en cuenta como bienes los bienes raíces, es decir, bienes inmuebles o que figuren en el registro de la propiedad.

Finalmente, el cliente podrá finalizar el proceso de elaboración del testamento y la propia red descentralizada se encargará de registrar y firmar dicho testamento como una transacción en un bloque de la blockchain.

Por lo tanto, el proceso de elaboración del testamento con el modelo que se propone en este proyecto quedaría tal y como se muestra en *Ilustración 6* en comparación con el modelo tradicional *Ilustración 5*.



Ilustración 6. Proceso de elaboración de Testamento con el modelo propuesto

Cabe destacar que para que este modelo funcione, la red de blockchain debe conectarse al Registro de la Propiedad para obtener los datos de las propiedades de los clientes y así estos puedan asignar a cada propiedad uno o varios herederos. Como ya vimos en el *Capítulo 3*, existe un proyecto [27] en Chile de la inmobiliaria Madesal y la startup Plexus que, entre otros objetivos, buscan crear un Registro de la Propiedad. Para este proyecto, no tiene sentido que se intente implantar este modelo sin que existiera antes un Registro de la Propiedad en

la red de blockchain por lo que se ha optado por desarrollar un pequeño Registro de la Propiedad basado en blockchain y Smart Contracts, aunque también se podría simular este registro con una base de datos relacional. Se verá en más detalle en el apartado 5.2 de diseño.

5.1.2 ANÁLISIS DEL PROCESO DE HERENCIA

El proceso de Herencia comienza con la defunción de un cliente y se extiende hasta que sus bienes han sido dispuestos o traspasados a los herederos que este había nombrado en su último testamento. Cabe la posibilidad que una persona no haya otorgado ningún testamento durante su vida, este tipo de sucesión se denomina intestada, ver [28, Ch. 3], casuística que no se ha tenido en cuenta en este proyecto pues si se da, los ascendientes, descendientes o colaterales deben proceder mediante vía judicial por una demanda que daría lugar a trámite en juicio y a una investigación para recopilar la masa hereditaria y fallar a favor o en contra de los solicitantes. Es un caso de uso que dista del objetivo de este trabajo fin de grado por lo que no se ha tratado.

Los pasos de los que consta el proceso de herencia se pueden dividir en cuatro:

1. **Defunción:** Cuando una persona fenece, un médico o forense se encarga de elaborar el certificado médico de defunción. Este certificado es un informe clínico donde el facultativo expresa en términos médicos la defunción y razón de ella. A partir de este informe médico de defunción se elabora el Certificado de Defunción del Registro Civil, documento legal con validez jurídica que hace constar la defunción de la persona junto con la hora, lugar, y otros datos.
A partir de ese momento, quedan bloqueados durante quince días laborables los bienes de difunto para evitar un uso fraudulento de ellos.
2. **Acudir al Ministerio de Justicia:** Pasados los quince días laborables, un ascendiente, descendiente o colateral, acude al Ministerio de Justicia a solicitar el Certificado de Últimas Voluntades que se expide a partir del Certificado de Defunción del Registro Civil. En el Certificado de Últimas Voluntades figuran los datos del difunto como la fecha de nacimiento, fecha de defunción y, además, todos los testamentos que ha otorgado o no en vida.

3. **Acudir al Notario:** Con el Certificado de Últimas Voluntades, se acude al notario el cual se encarga, a partir del último testamento que figura en el Certificado de Últimas Voluntades, de reunir toda la masa hereditaria y a todos los herederos nombrados.
4. **Reunión del notario y herederos:** Se celebra una reunión con el notario y los herederos presentes. En dicha reunión el notario lee el testamento en presencia de los sucesores, se les informa de lo que les corresponde, y estos deciden si aceptan o renuncian a la herencia.

A continuación, en la *Ilustración 7* se muestra un diagrama que refleja los pasos principales para llevar a cabo el proceso de herencia.



Ilustración 7. Proceso de Herencia con el modelo tradicional

A partir de estos cuatro pasos, se busca una adaptación para que la aplicación a desarrollar pueda realizar el mismo proceso.

En primer lugar, sí será necesario que un facultativo elabore el Certificado Médico de Defunción para que en este nuevo modelo quede registrado la defunción de la persona en cuestión. Ese hecho será, al igual que en el modelo tradicional, el que desencadene el inicio de todo el proceso de herencia.

Una vez registrado el Certificado Médico de Defunción, automáticamente se consultará cual es el último testamento en el Certificado de Últimas Voluntades del difunto y se notificará a los herederos designados en dicho testamento el fallecimiento de la persona junto con las propiedades que le corresponden. Los herederos entonces podrán aceptar o renunciar a la herencia que se les indica de tal forma que cuando todos hayan decidido, o bien cuando el Ministerio de Justicia lo deseé, se ejecutará el testamento y automáticamente se realizarán las modificaciones pertinentes en el registro de la propiedad para cambiar a los propietarios de los inmuebles y sustituir al testador por los herederos.

El proceso de herencia en el nuevo modelo no requerirá de más pasos. El modelo tradicional requería de más trámites y gestiones para asegurar la transparencia y confiabilidad en el proceso, depositando esta sobre el notario. Al hacer uso de la tecnología de Blockchain, el proceso se realiza con mayor transparencia y depositando la confiabilidad sobre la red descentralizada sin un control central y, por lo tanto, no hay que preocuparse de los trámites que evitan un traspaso irregular de los bienes, ya que el testamento será incorruptible.

A continuación, en la *Ilustración 8* se muestra un diagrama de como quedaría el nuevo modelo del proceso de herencia desarrollado en este trabajo fin de grado comparado con el modelo tradicional de la *Ilustración 7*.



Ilustración 8. Proceso de Herencia con el nuevo modelo propuesto

Cabe destacar que para poder registrar los Certificados Médicos de Defunción se necesita un Registro Civil, el cual, al igual que con el Registro de la Propiedad, se ha decidido desarrollar e implantar un pequeño Registro Civil basado en la tecnología de Blockchain y Smart Contracts. Se puede ver en más detalle en el apartado 5.2 sobre el diseño.

5.1.3 REQUISITOS DE DISEÑO OBTENIDOS

Como conclusión, ante el análisis realizado para el proceso de elaboración de testamentos y el proceso de herencia se han obtenido unos requisitos que necesita el modelo propuesto para que pueda ser funcional.

- En primer lugar, se necesita, como ya se ha indicado, desarrollar un Registro de la Propiedad donde poder almacenar en la red de blockchain las distintas propiedades inmuebles.
- Se necesita desarrollar un Registro Civil donde se puedan almacenar los Certificados Médicos de Defunción.

Tanto la red de blockchain como la tecnología de Smart Contract basa su funcionamiento en algoritmos asimétricos con claves públicas y privadas, por lo que cada contrato desplegado o usuario que participa en la red quedan identificados por una dirección de cuenta de la red de blockchain, en este caso Ethereum. Actualmente en España se usa el Documento Nacional de Identidad (DNI) para identificar a cada ciudadano, pero al usar cuentas en la red de blockchain no tendría sentido almacenar en la red un registro de DNIs cuando la red ya puede usar como identificador único la cuenta de los usuarios y, además, en España, ya existe un registro de DNIs en el Centro de Proceso de Datos por lo que:

- Se requiere de una infraestructura que permita identificar a cada ciudadano con su cuenta en la red de blockchain, por lo tanto, se ha diseñado una base de datos relacional que simula el Centro de Proceso de Datos para poder identificar a cada ciudadano con su DNI y también con una cuenta de la red de blockchain Ethereum.

La aplicación debe ser capaz de reproducir los procesos mostrados en *Ilustración 5. Proceso de elaboración de Testamento con modelo tradicional* e *Ilustración 7. Proceso de Herencia con el modelo tradicional* a partir de los nuevos modelos que se ven en *Ilustración 6. Proceso de elaboración de Testamento con el modelo propuesto* e *Ilustración 8. Proceso de Herencia con el nuevo modelo propuesto* por lo que:

- Se necesita una lógica que funcione sobre la red de blockchain con la tecnología de Smart Contract que permita
 - Reproducir los procesos de elaboración de testamento y de herencia.
 - Esta lógica debe permitir también almacenar en la red de blockchain el Certificados de Últimas Voluntades de cada cliente

- Además, debe de almacenar y vincular a estos certificados todos los testamentos que los clientes realicen.
- Esta lógica debe poder comunicarse con el Registro de la Propiedad para listar los inmuebles de los que disponen los testadores.
- Debe también poder comunicarse con el Registro Civil para poder iniciar el proceso de herencia cuando una persona fallece.
- Los testadores deben poder escribir tantos testamentos como deseen, asignando a cada propiedad uno o varios herederos y el porcentaje de dicha propiedad que desea que le correspondan a cada sucesor.
- La aplicación debe permitir a los futuros herederos aceptar o renunciar las herencias en las que se le han nombrado cuando el testador fenece y no antes de ello.
- Una vez que todos los herederos nombrados han aceptado o renunciado a la herencia de un testador, la lógica de la aplicación debe ser capaz de recalcular los porcentajes asignados si una o más persona renuncian a su herencia repartiendo el porcentaje total de renuncia entre el resto de los herederos de forma proporcional a su relación asignada en origen por el testador.
- También la lógica de la aplicación deber permitir la ejecución un testamento cuando todos los herederos han aceptado o renunciado a la herencia, modificando los propietarios y porcentajes de propiedad en el Registro de la Propiedad.
- Finalmente, no se podrá ejecutar varias veces un testamento para una persona fallecida.

Por último, respecto a la gestión y administración de perfiles de usuarios y control de acceso a la aplicación:

- No se va a realizar un control de acceso pues para interactuar con una red de blockchain, en es te caso Ethereum, se necesita una cuenta en dicha red con criptomonedas y sin ella no se pueden realizar transacciones. Para que los clientes puedan interactuar con la red de Ethereum a partir de sus cuentas, en este caso, se

usará un monedero de criptomonedas, MetaMask que permite a los usuarios firmar transacciones con sus cuentas. Para tener una cuenta y firmar en la red de Ethereum, a través de MetaMask u otro monedero, es necesario iniciar sesión con la cuenta del monedero por lo que los monederos y las cuentas ya actúan como control de acceso quedando los usuarios identificados y autenticados por sus cuentas de la red descentralizada.

- Se van a diseñar dos interfaces distintas:
 - Una interfaz común para todos los usuarios donde podrán crear sus testamentos y gestionar sus notificaciones.
 - Una interfaz para administrar el Registro de la Propiedad y el Registro Civil la cual solo podrán interactuar las cuentas o usuarios autorizados.

Estos requisitos obtenidos del análisis de ambos procesos permitirán realizar un diseño mostrado en el siguiente apartado, 5.2, para el desarrollo de la aplicación.

5.2 DISEÑO

Ante el análisis realizado en el apartado 5.1 se ha realizado un diseño partiendo de los requisitos obtenidos en 5.1.3. Para poder desarrollar la aplicación de una forma estructurada, en primer lugar, con el fin de que nuestro modelo pueda funcionar correctamente, se ha elaborado un diseño de la arquitectura que tendrá el sistema. A continuación, se ha planteado varios diagramas de caso de uso que permitirá comprender las acciones por las que los usuarios podrán interactuar con la aplicación. Para comprender la estructura del software y el funcionamiento de este, se han diseñado un diagrama de clases junto con varios diagramas de secuencia para el desarrollo de las diferentes funcionalidades. Finalmente, se presentará el diseño del *front-end* modelo donde los usuarios podrán interactuar con la aplicación

5.2.1 DISEÑO DE ARQUITECTURA

En primer lugar, se ha diseñado una arquitectura en la que se implantará el modelo a desarrollar. Dicha arquitectura se muestra a continuación en la *Ilustración 9*.

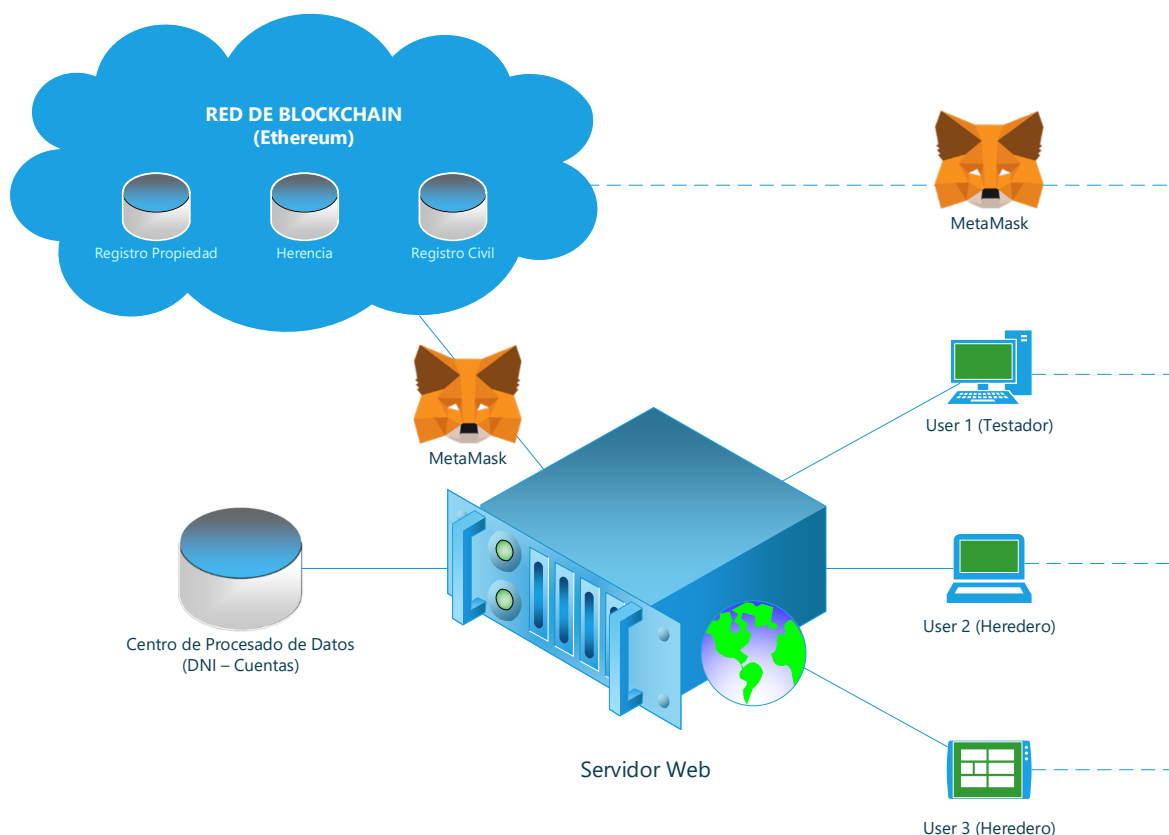


Ilustración 9. Diagrama de la arquitectura del sistema

Como podemos ver en el diagrama, la infraestructura consta de cuatro elementos básicos:

- **Red de Blockchain (Ethereum):** Se trata de la red donde se encuentra el *back-end* de la aplicación y donde se almacenará los datos del Registro de la Propiedad, Registro Civil y datos del proceso de herencia. Sobre los nodos de esta red se ejecutará la lógica de la aplicación.
- **Centro de Proceso de Datos:** Es una base de datos que contiene los DNIs de los ciudadanos y una vinculación a los números de cuenta de blockchain (Ethereum). Simula el Centro de Procesado de Datos de España, y aunque en este centro hay más datos, en este caso solo se emulan los necesarios.
- **Servidor web:** En él se almacena la aplicación web, aunque en realidad solo *el front-end* pues el *back-end* se encuentra almacenado en la propia blockchain. Permite

actuar de intermediario para algunas operaciones entre la red de blockchain y el Centro de Procesado de Datos.

- **Otros elementos:**

- **Usuarios:** Podrán conectarse a la aplicación web a través del servidor web y a la red de blockchain directamente.
- **MetaMask:** Monedero de criptomonedas a través del cual, el navegador web y los clientes pueden comunicarse con la red de blockchain.

Sobre esta arquitectura, se implanta el modelo a desarrollar. Teniendo la arquitectura modelada, es necesario para el diseño del software, expresar las funcionalidades de la aplicación y las interacciones que podrán tener los usuarios con ella, para ello, se realizan unos diagramas de caso de uso.

5.2.2 DIAGRAMAS DE CASOS DE USO

Con el fin de capturar los requisitos funcionales y poder expresarlos desde el punto de vista del usuario, se han realizado dos diagramas de caso de uso para modelar las interacciones de los usuarios con el sistema.

En primer lugar, en *Ilustración 10. Diagrama de casos de uso del actor Cliente* se puede ver el diagrama de caso de uso del usuario cliente cuyo rol es de testador y posible heredero.

En este caso de uso se representa las interacciones que el actor cliente podrá tener con el sistema. Estas tres interacciones son:

- **Consultar CUV:** Los clientes podrán consultar su Certificado de Últimas Voluntades que, aunque en este proyecto solo contendrá datos personales y testamentos, en trabajos futuros podrá contener más información como testamentos vitales, donaciones u otros. La consulta del Certificado de Últimas Voluntades incluye la funcionalidad de consultar Testamentos que el usuario ha otorgado, al igual que la consulta de los Traspasos dentro de cada Testamento.

- **Crear Testamento:** Los clientes podrán crear testamentos desde la aplicación y una vez creados, podrán asignar porcentajes de sus propiedades a los futuros herederos y firmar el testamento.
- **Consulta de Trámites:** los clientes podrán consultar trámites pendientes o realizados respecto a las diferentes herencias en las que han sido designados como herederos. También podrán aceptar y renunciar a las herencias cuando un testador que les había nombrado herederos fallece.

Véase el diagrama de a continuación:

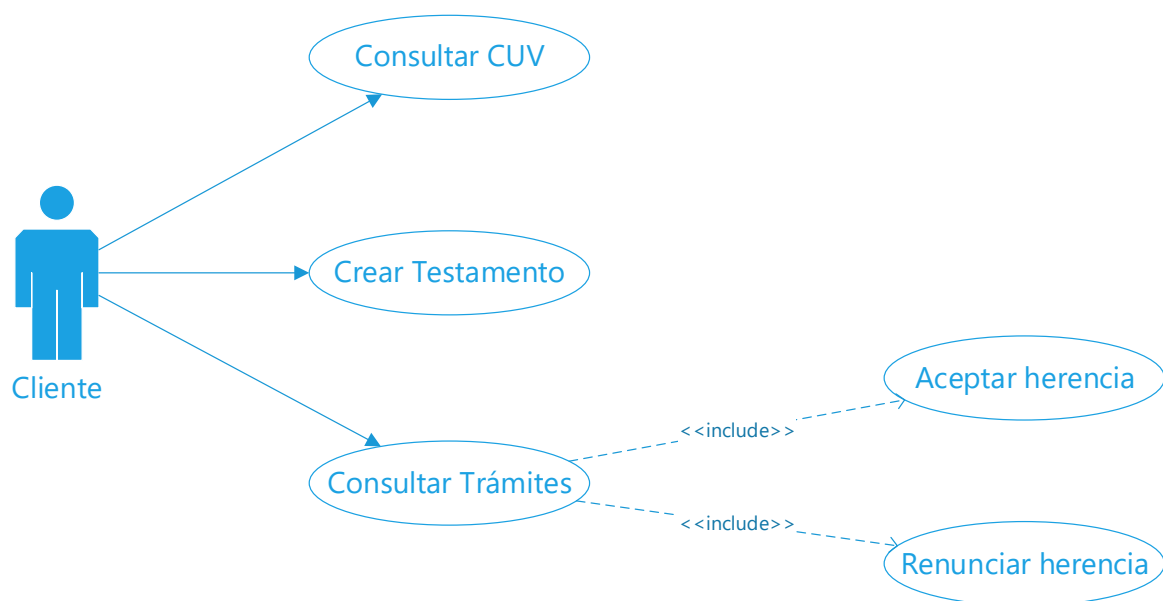


Ilustración 10. Diagrama de casos de uso del actor Cliente

En segundo lugar, se presenta el diagrama de casos de uso del usuario Ministerio en *Ilustración 11. Diagrama de casos de uso del actor Ministerio*

En este caso de uso se representa las interacciones que el actor Ministerio podrá tener con el sistema, estas interacciones son:

- **Añadir finca al Registro de la Propiedad:** El Ministerio podrá rellenar los datos de una finca y añadir dicho bien al Registro de la Propiedad.

- **Consultar finca en el Registro de la Propiedad:** El Ministerio podrá consultar la información de una determinada finca en el Registro de la Propiedad a través de un Idufir. Esto simula a una nota simple del Registro de la Propiedad.
- **Añadir CMD al Registro Civil:** El Ministerio podrá añadir un Certificado Médico de Defunción al Registro Civil cuando una persona fallezca.
- **Consultar CMD en el Registro Civil:** El Ministerio podrá consultar un Certificado Médico de Defunción, a través del Documento Nacional de Identidad de una persona.
- **Ejecutar Testamento:** El Ministerio podrá ejecutar el testamento de una persona a partir del Documento Nacional de Identidad. El Ministerio solo dará la orden, el proceso será llevado a cabo por la propia aplicación comprobando que existe un Certificado Médico de Defunción como se verá más adelante en *Ilustración 21. Diagrama de secuencia del proceso de herencia (II)*.

A continuación, se muestra el diagrama de caso de uso del actor Ministerio:

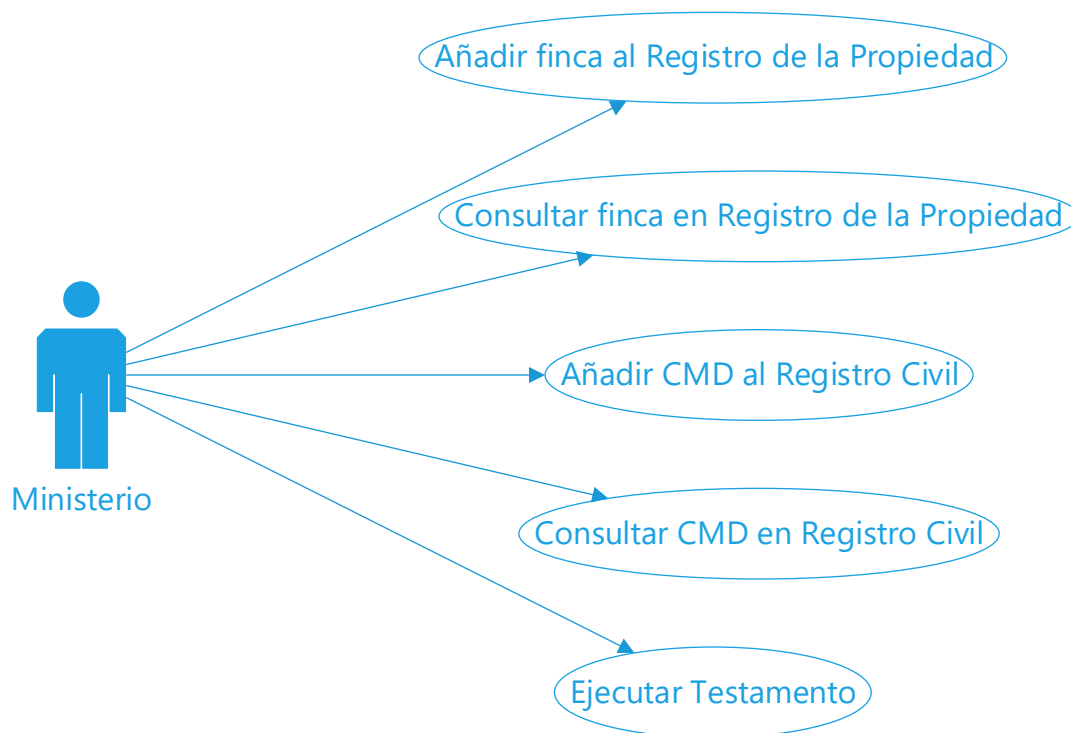


Ilustración 11. Diagrama de casos de uso del actor Ministerio

Una vez establecido los casos de uso para los posibles actores que interactuarán con la aplicación, es necesario saber cómo estarán organizados los datos de los distintos Certificados de Últimas Voluntades de cada cliente y los distintos Testamentos que cada cliente otorgue con los diferentes Traspasos.

5.2.3 ESTRUCTURA DE DATOS PRINCIPAL

Para comprender mejor como se van a estructurar los datos de los Certificados de Últimas Voluntades, Testamentos y Traspasos, se va a definir cada término y mostrar un diagrama de la estructura de los datos:

- **Certificado de Últimas Voluntades (CUV):** Será una estructura de datos que simulará a un Certificado de Últimas Voluntades real. En el figuran datos personales del cliente y cabe destacar los siguientes datos que figuran en la estructura:
 - Id CUV: será el id del Certificado de Últimas Voluntades. Este Id se generará a partir del número entero que resulta de del cómputo de hash de Ethereum SHA-3(Keccak-256) de la concatenación de la cuenta del cliente al que se le crea el CUV y una estampa del tiempo de la fecha de creación del CUV. Esto evita que nunca se genere el mismo ID de CUV para dos clientes distintos.
 - Ids de testamentos: Consiste en un array con todos los Id de los diferentes Testamentos que el cliente otorga. Simplemente contiene el id, para referenciarlo, no el testamento entero. Actúa como identificador único del CUV
- **Testamento:** Estructura de datos que simula un Testamento real. Incluye algunos datos que corresponden al cliente que otorga dicho testamento. Los datos más importantes que caben destacar son:
 - Id Testamento: será el id del Testamento que se genera a partir del número entero que resulta del cómputo de hash de Ethereum SHA-3(Keccak-256) de la concatenación del Id CUV del cliente, la cuenta del cliente y la estampa de tiempo de la fecha en la que se generó el testamento. Actúa como único identificador del testamento.

- Ids de traspasos: Consiste en un array de los ids de los traspasos de inmuebles a herederos que designa el testador. Es un array con lo ids, no contiene los datos del traspaso en sí.
- **Traspaso/Asignación**: Estructura de datos que detalla el traspaso que recoge un testamento de una propiedad y el heredero o conjunto de herederos de dicha propiedad junto con los porcentajes que les corresponden. Los datos más importantes que destacar son:
 - Id Traspaso: será el id del Traspaso que se genera a partir del número entero que resulta del cómputo de hash de Ethereum SHA-3(Keccak-256) de la concatenación del Id del testamento al que pertenece y del Idufir de la propiedad que se va a traspasar. Actúa como único identificador del traspaso.
 - Propietarios destino: Array con las cuentas de los herederos de la propiedad a la que corresponde el traspaso
 - Porcentajes destino: Porcentajes que les corresponde a cada heredero de la propiedad del correspondiente traspaso.

En la *Ilustración 12* se presenta un diagrama con la estructura de los datos mencionados.

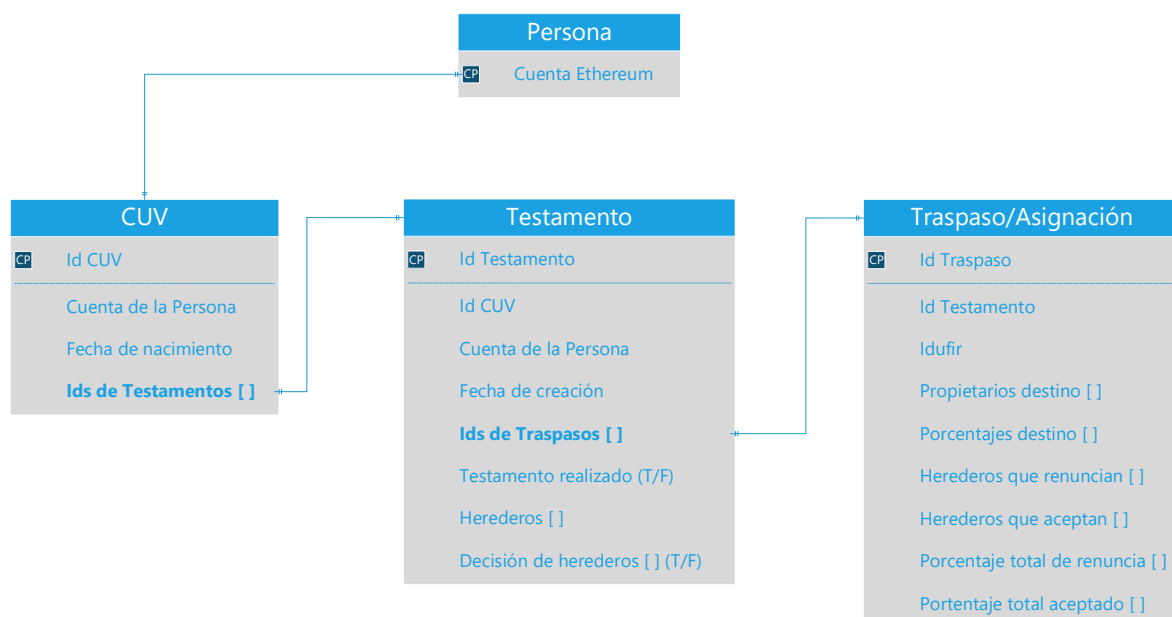


Ilustración 12. Diagrama de estructura de datos

5.2.4 DIAGRAMA DE CLASES

Realizado el diseño de la arquitectura y teniendo en cuenta los casos de uso definidos para cada actor y la estructura de datos del modelo que se está planteando, se establece un diseño de alto nivel de la estructura del *back-end* de la aplicación.

En el paradigma de la programación de Smart Contract con Solidity, no existen clases como tal, sino que cada contrato es un script que incluye atributos o variables globales que se almacenan en la blockchain cuando se declaran y métodos o funciones cuya lógica permite interactuar y realizar operaciones con las variables globales o variables internas de las funciones.

Para poder entender la relación e interacción entre los contratos o scripts programados se ha realizado un diagrama de clases, que en vez de representar clases representará los contratos a desplegar de la aplicación desarrollada. El diagrama consta de tres contratos que interactúan entre sí con varias interfaces:

- **RegistroPropiedad.sol:** Contrato que simula el Registro de la Propiedad. Consta de una estructura, Finca, formada por los datos que caracterizan la definición de una propiedad.
- **RegistroCivil.sol:** Contrato que simula el Registro Civil. Consta de una estructura, CMD, que contiene los datos que definen un Certificado Médico de Defunción.
- **Herencia.sol:** Contrato que contiene toda la lógica de programación del proceso de elaboración de testamentos y de herencia. Contiene tres estructuras que ya se han detallado en el apartado *Estructura de datos principal* y permite acceder a cada instancia de dichas estructuras a través de tres mapeos diferentes.

Cabe destacar que Herencia.sol interactúa con RegistroPropiedad.sol a través de una interfaz que permite transferir propiedades de un usuario a otro cuando se produce una herencia. De igual manera Herencia.sol y RegistroCivil.sol interactúan a través de dos interfaces que permite a Herencia.sol consultar fechas de nacimiento y defunción de un cliente y a RegistroCivil.sol consultar los herederos de un testamento. Ver diagrama en *Ilustración 13*.

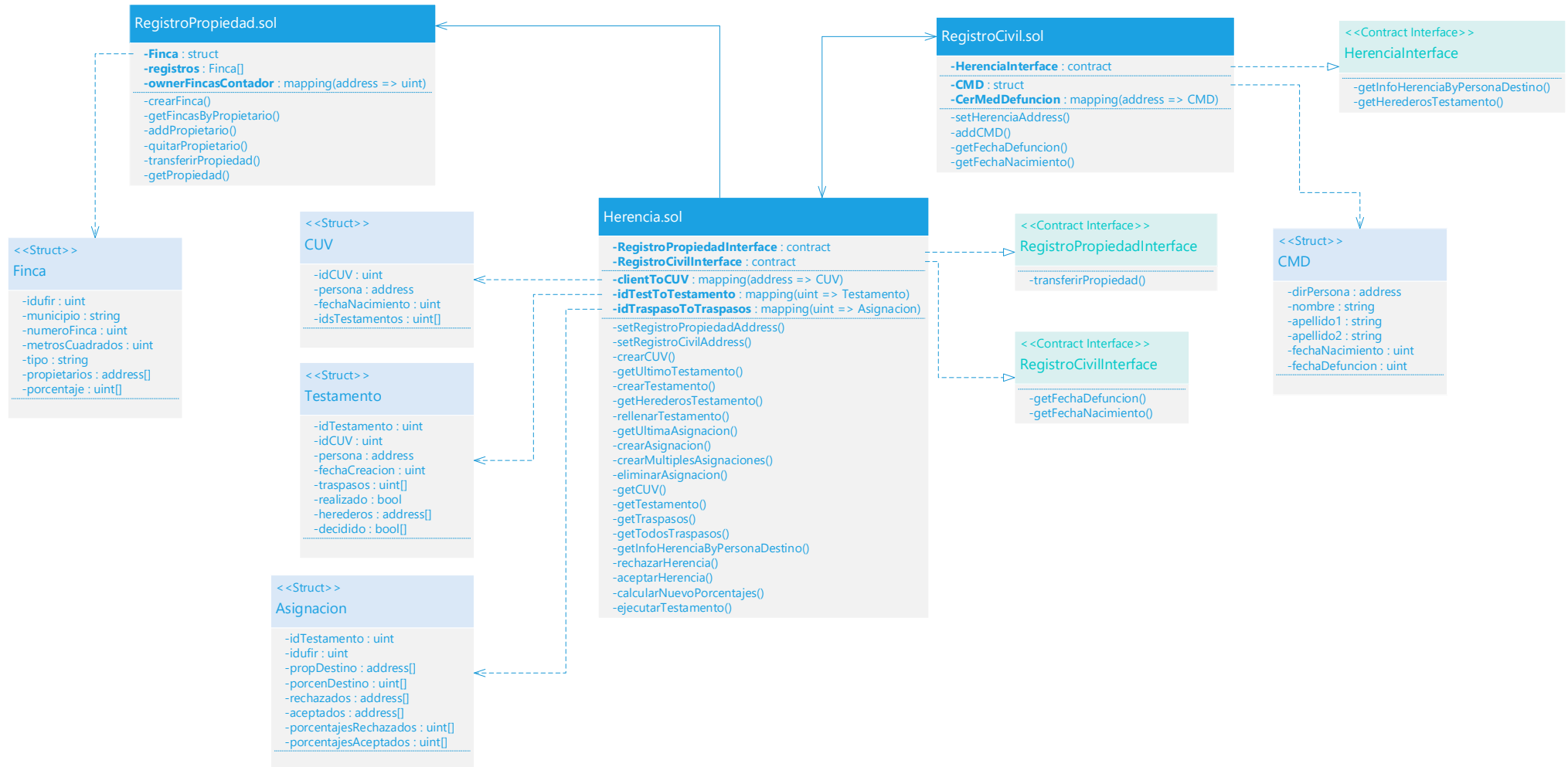


Ilustración 13. Diagrama de clases del modelo propuesto

5.2.5 DIAGRAMAS DE SECUENCIA

Hasta aquí, queda diseñada toda la estructura de la aplicación, pero es necesario tener un diseño funcional de ella y conocer cómo se realizarán las interacciones de los usuarios con la aplicación y la red de blockchain. Para ello se ha realizado una serie de diagramas de secuencia donde se detalla la interacción de los componentes a través del tiempo, haciendo énfasis en la secuencia de los mensajes y su orden temporal. Cabe destacar que en todos los diagramas el servidor web se comunica con la red de blockchain a través de MetaMask.

Diagramas de secuencia de RegistroPropiedad.sol

En primer lugar, se muestran los diagramas de secuencia que corresponden al script RegistroPropiedad.sol, en el que se diferencian dos funcionalidades destacables.

La primera de ellas se trata de la creación de fincas, en *Ilustración 14* se muestra como el usuario Ministerio interactúa con la aplicación y la interacción entre el servidor web y la red de blockchain para registrar una finca en el Registro de la Propiedad.

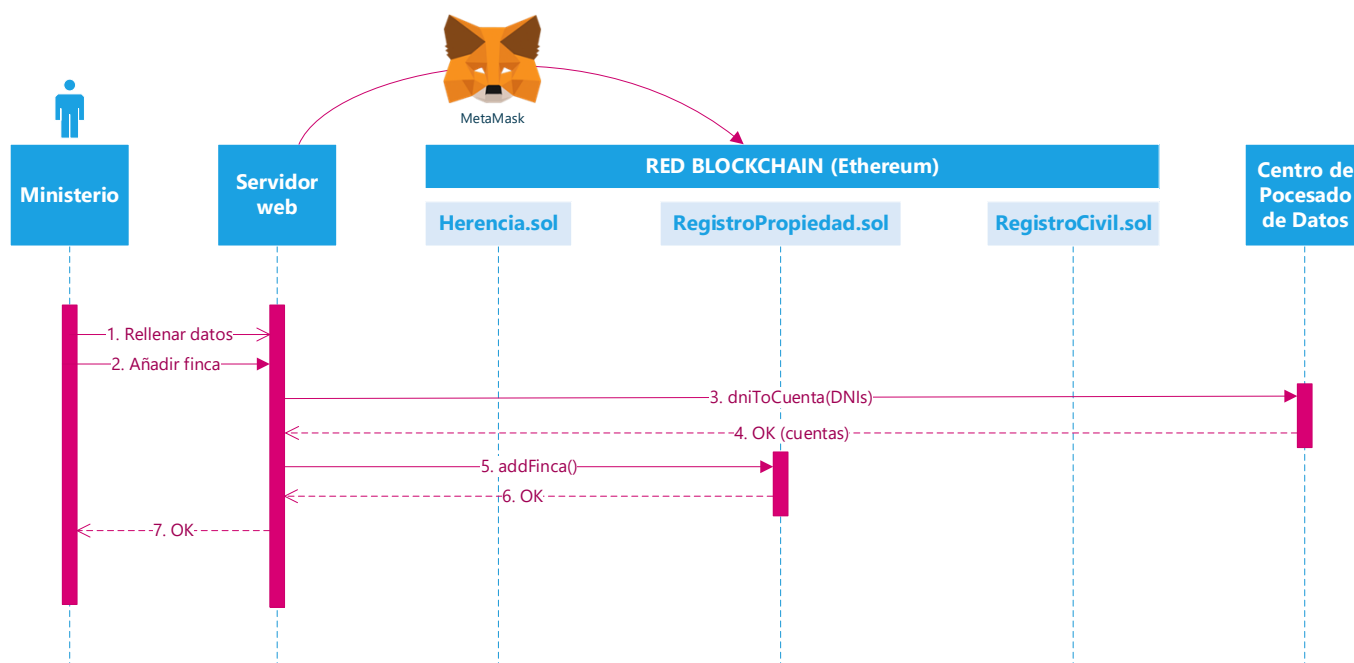


Ilustración 14. Diagrama de secuencia para la creación de fincas

La segunda funcionalidad que se muestra mediante un diagrama de secuencia puede verse en Ilustración 15 y se trata de la consulta de fincas registradas en el Registro de la Propiedad.

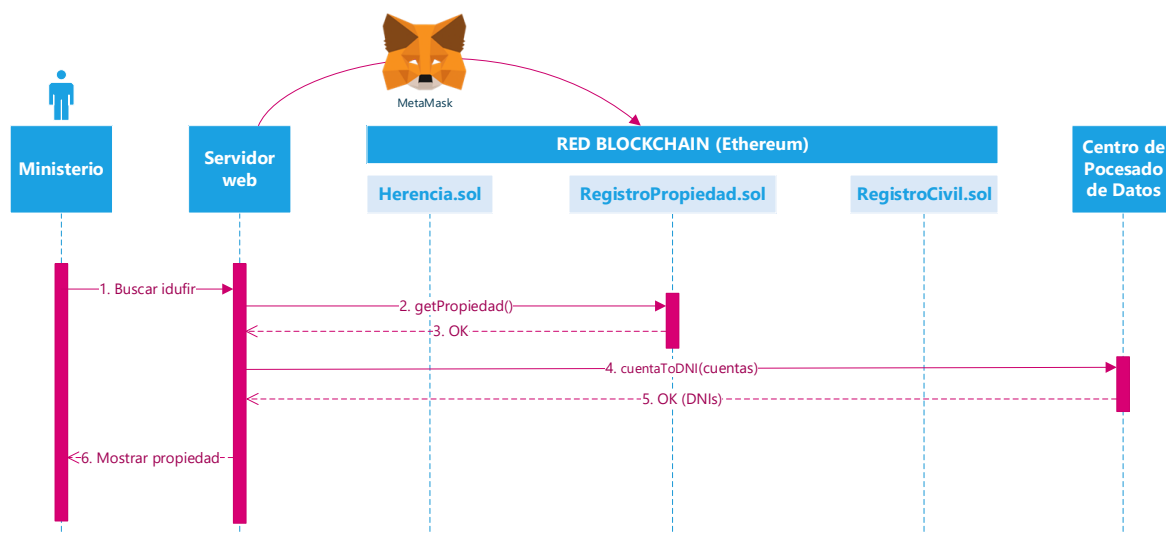


Ilustración 15. Diagrama de secuencia de consulta de fincas

Diagramas de secuencia de RegistroCivil.sol

A continuación, se muestran los diagramas de secuencia que corresponden con dos funcionalidades del script RegistroCivil.sol. El primero de ellos se trata de la creación de un Certificado Médico de Defunción (CMD), dicho diagrama puede verse en Ilustración 16.

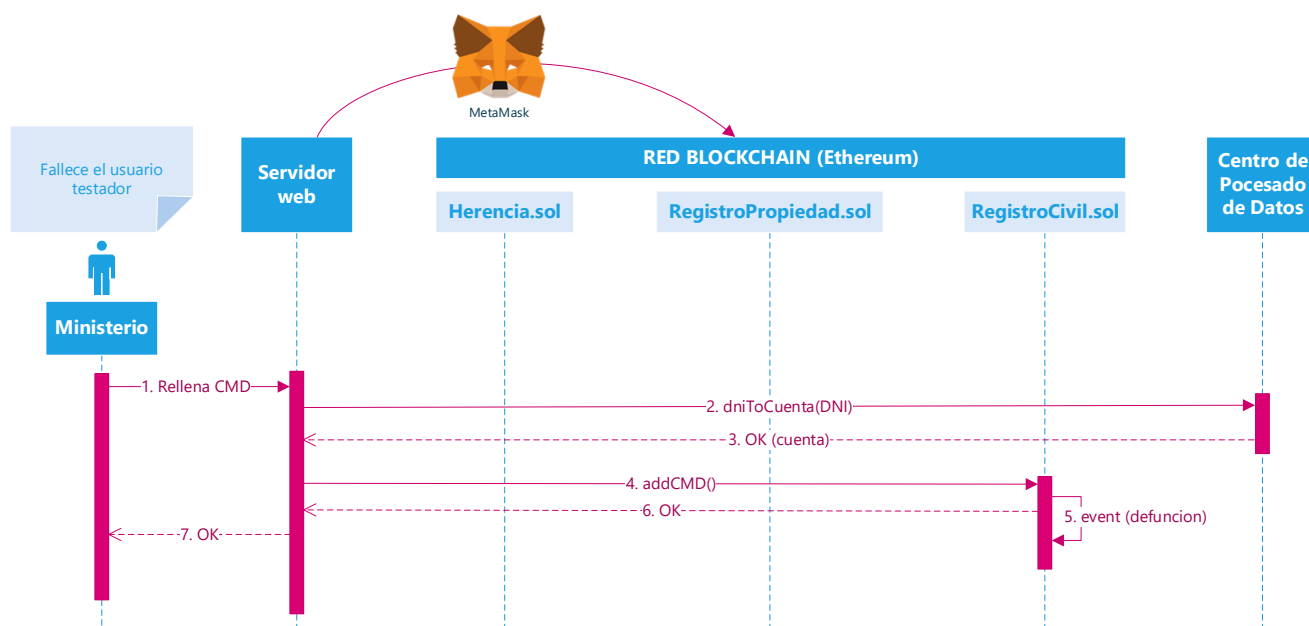


Ilustración 16. Diagrama de secuencia de la creación de un CMD

La segunda funcionalidad se muestra en *Ilustración 17* y se trata de la consulta de un Certificado Médico de Defunción (CMD) en el Registro Civil.

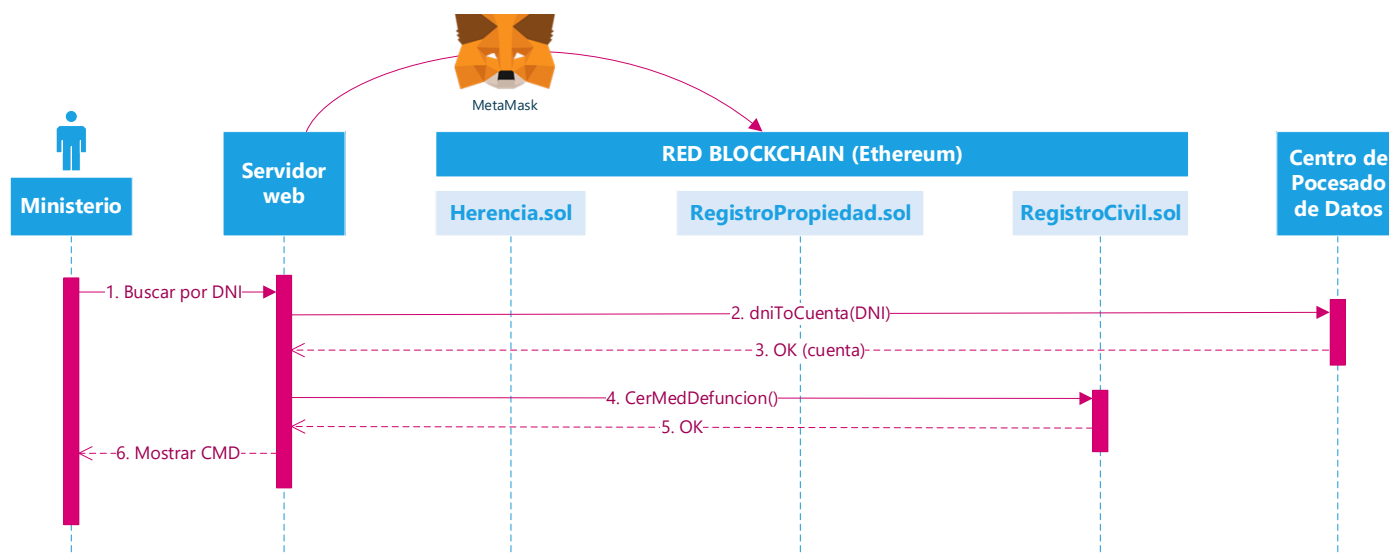


Ilustración 17. Diagrama de secuencia de la consulta de un CMD

Diagramas de secuencia de Herencia.sol

Finalmente, se muestran los diagramas de secuencia que corresponden con las funcionalidades del script Herencia.sol. Este script contiene las funcionalidades principales de este trabajo fin de grado por lo que se explicará más en detalle cada uno de los diagramas.

El primero de ellos se trata de la escritura de un testamento y se muestra en *Ilustración 18. Diagrama de secuencia de escritura de Testamento*. El usuario podrá crear un testamento (1) y el servidor se encargará de ejecutar la función (2) de Herencia.sol para crearlo. Después, Herencia.sol consultará en RegistroPropiedad.sol las propiedades que posee el usuario (5), con el fin de que el servidor pueda mostrarlas en el *front-end* al usuario (7). A continuación, el usuario podrá asignar a cada propiedad el número de herederos que desee y asignarles un porcentaje de herencia a cada uno (8). Cuando el usuario desee firmar el testamento (9) el servidor consulta con el Centro de Procesado de Datos las cuentas de los herederos, las traduce (10 y 11) y rellena el último testamento (12) creando las asignaciones (14) que se han especificado en el *front-end* en (8). Finalmente, el testamento queda escrito (16). Aunque el testamento en un primer momento esté vacío cuando se crea en (1), se puede cortar o abortar la operación antes de llegar a la firma del testamento (9), esto se ha diseñado así para

dejar constancia en la red la intención por parte de un testador de escribir testamento, aunque quede sin rellenar.

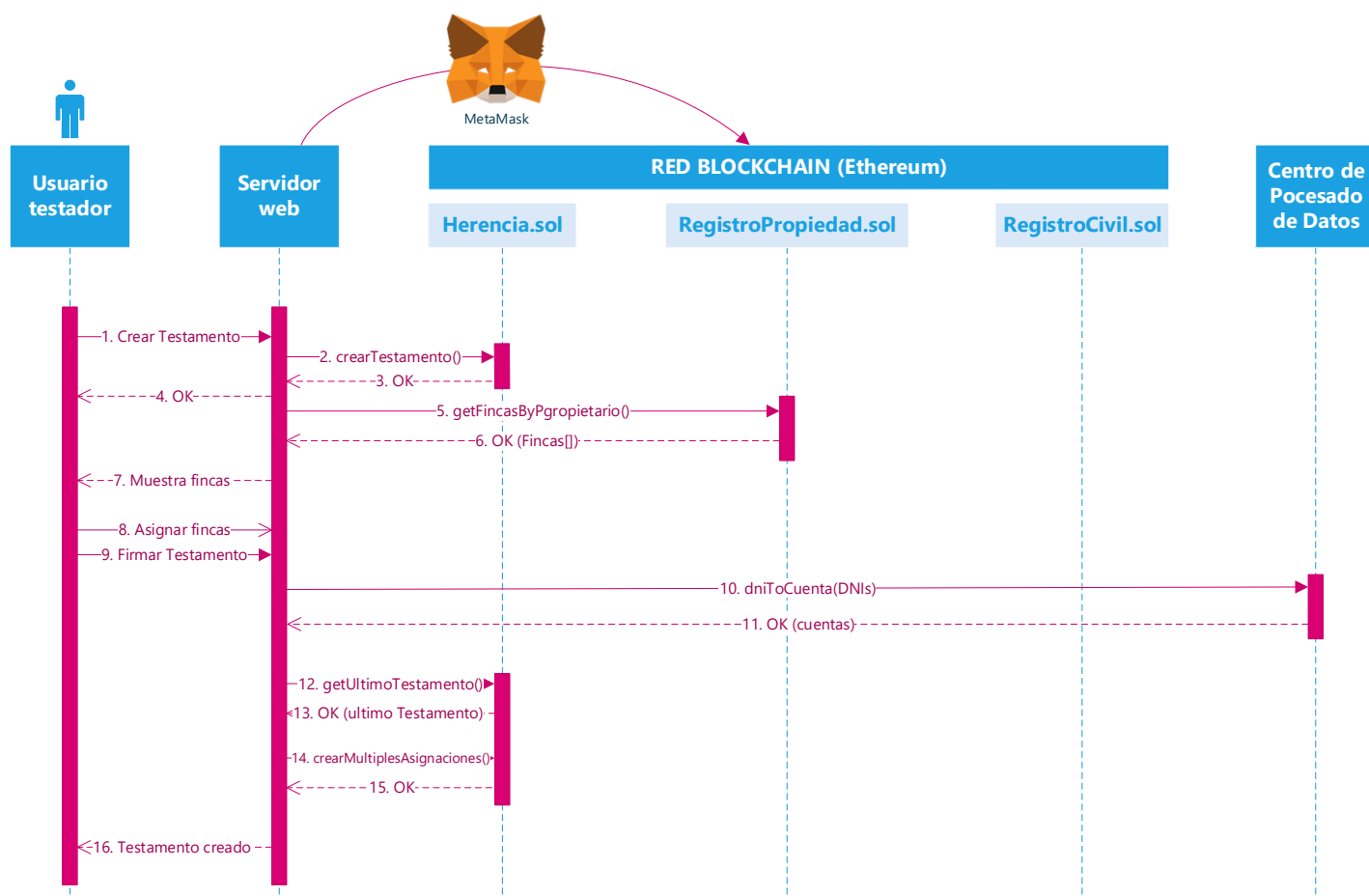


Ilustración 18. Diagrama de secuencia de escritura de Testamento

La segunda funcionalidad modelada se trata de la consulta de un testamento, esta se muestra en *Ilustración 19. Diagrama de secuencia de la consulta de Testamentos*. La aplicación muestra automáticamente toda la información del Certificado de Últimas Voluntades (CUV) del cliente en el *front-end*, por lo que, cuando un usuario desea consultar un testamento basta con que este acceda a la web (1) y el servidor web consultará a Herencia.sol (2) el CUV de dicho cliente. El servidor traducirá mediante consultas al Centro de Procesado de Datos las cuentas que aparezcan en el CUV (4) convirtiéndolas en DNIs y cuando tenga todos los datos mostrará el CUV al cliente (6). Los clientes podrán seleccionar de un listado de testamentos del CUV el que deseen ver con mayor detalle y entonces el servidor web consultará dicho

testamento a Herencia.sol (8) y traducirá las cuentas de los herederos designados en el testamento a sus correspondientes DNIs (10) mostrando toda la información con detalle al usuario (12). Finalmente, de igual forma, el usuario podrá seleccionar un traspaso o asignación dentro de un testamento (13) y el servidor obtendrá los detalles de dicho traspaso (14) consultando a Herencia.sol y traduciendo las cuentas de los herederos a sus respectivos DNIs (16) para poder mostrar la información en detalle (18).

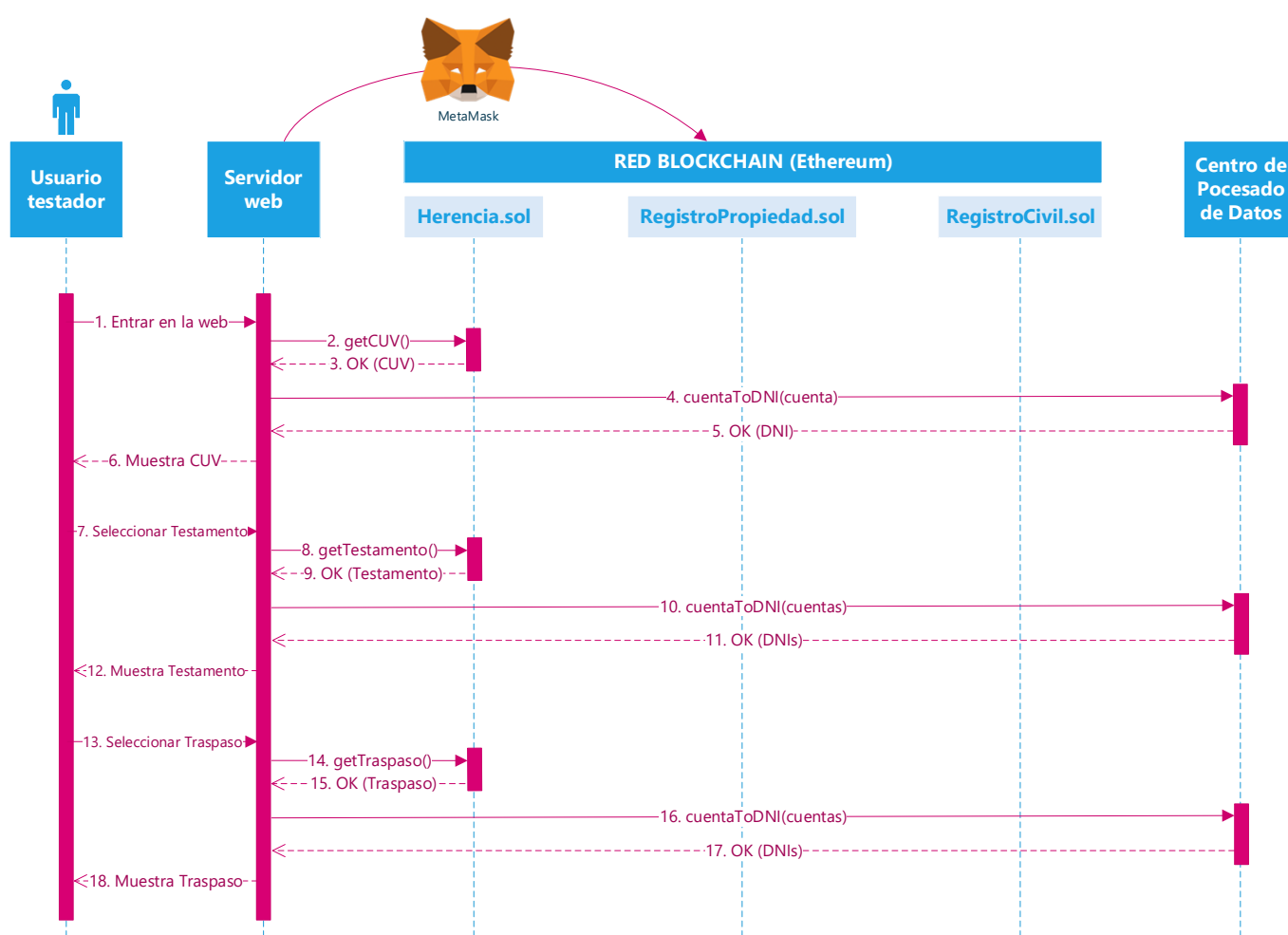


Ilustración 19. Diagrama de secuencia de la consulta de Testamentos

La tercera funcionalidad modelada se trata de la ejecución de una herencia. Esta funcionalidad se ha expresado en dos diagramas que pueden verse en *Ilustración 20. Diagrama de secuencia del proceso de herencia (I)* e *Ilustración 21. Diagrama de secuencia del proceso de herencia (II)*.

Cuando un usuario fallece, el Ministerio es el encargado de añadir en el Registro Civil el Certificado Médico de Defunción (CMD) por lo que rellena los datos del CMD (1) en la aplicación y el servidor web traduce el DNI del difunto para obtener la cuenta (2) y así poder añadir a RegistroCivil.sol el CMD (4). RegistroCivil.sol no solo añade el CMD a la cadena de bloques, sino que también emite un evento de la defunción (5) para notificar a los herederos el suceso. A continuación, los herederos cuando acceden a la aplicación (8), el servidor cargará los trámites pendientes por resolver (9) consultando los eventos de defunciones que han tenido lugar y filtrando dichos eventos por los que el usuario ha sido nombrado herederos (10). De igual forma, el servidor consulta los eventos resueltos (12) y así muestra al cliente en el *front-end* los trámites pendientes (14), trámites aceptados (15) y trámites rechazados (16). Los herederos podrán aceptar o renunciar a las herencias pendientes (17) y su decisión quedará registrada en Herencia.sol (18).

Cuando todos los herederos hayan aceptado o renunciado a la herencia, el ministerio podrá ejecutar el testamento (21) a partir del DNI de un difunto. El servidor web consultará cual es la cuenta que corresponde al DNI del difunto (22) y entonces el servidor podrá dar la orden ejecutar el testamento (24) a Herencia.sol que ejecutará el ultimo testamento de la persona difunta después de obtener la fecha de defunción (25), la fecha de nacimiento (27) y comprobar que la fecha de defunción es posterior a la fecha del último testamento y la fecha de nacimiento que figura en el CUV es la misma que en el CMD de RegistroCivil.sol (29). Herencia.sol realizará un cálculo de porcentajes, pues habrá herederos que puedan haber renunciado a la herencia y dicho porcentaje se repartirá de forma proporcional entre el resto de los herederos que han aceptado (30). Finalmente Herencia.sol manda la instrucción de transferencia de propiedades (31) a RegistroPropiedad.sol.

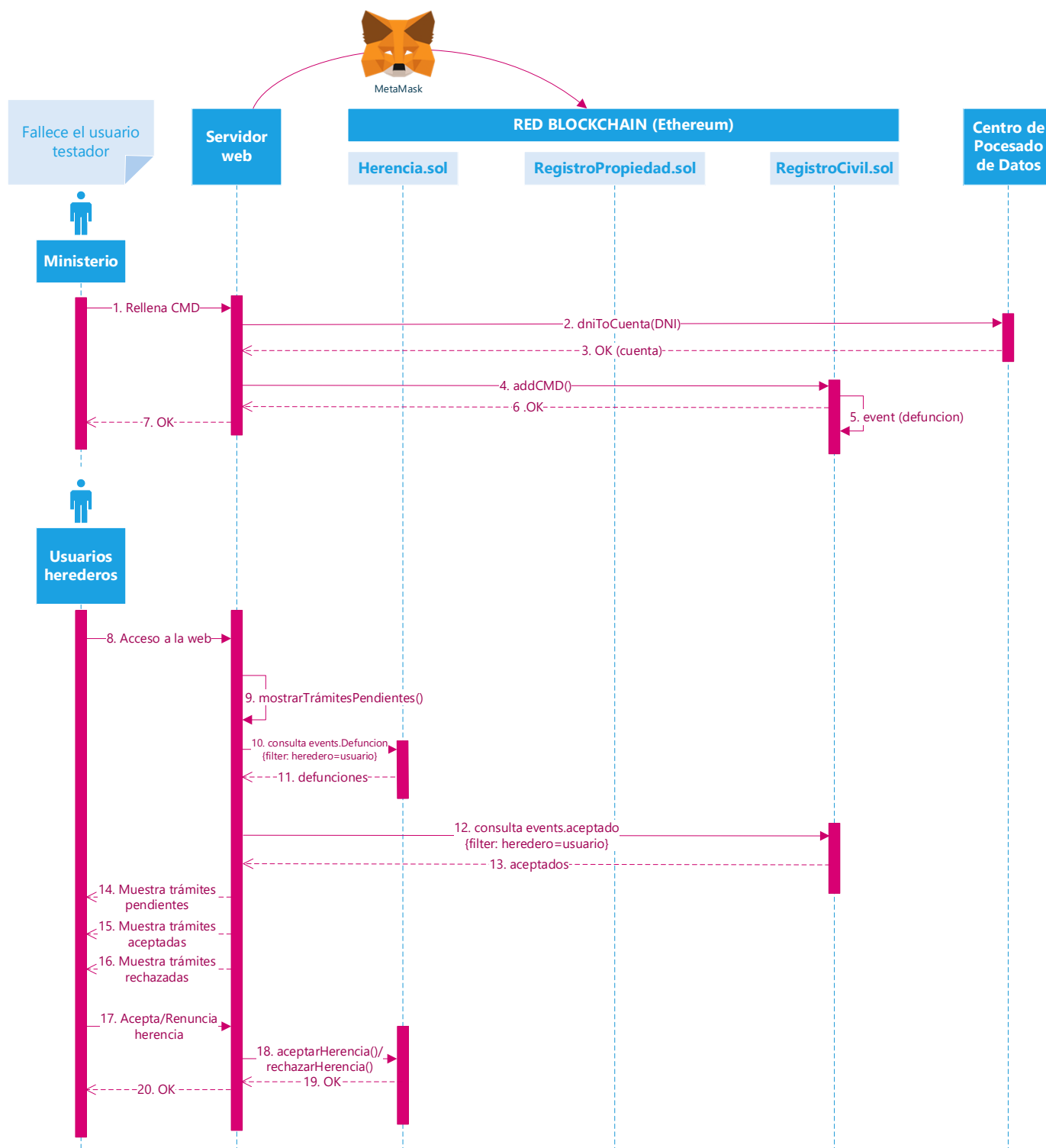


Ilustración 20. Diagrama de secuencia del proceso de herencia (I)

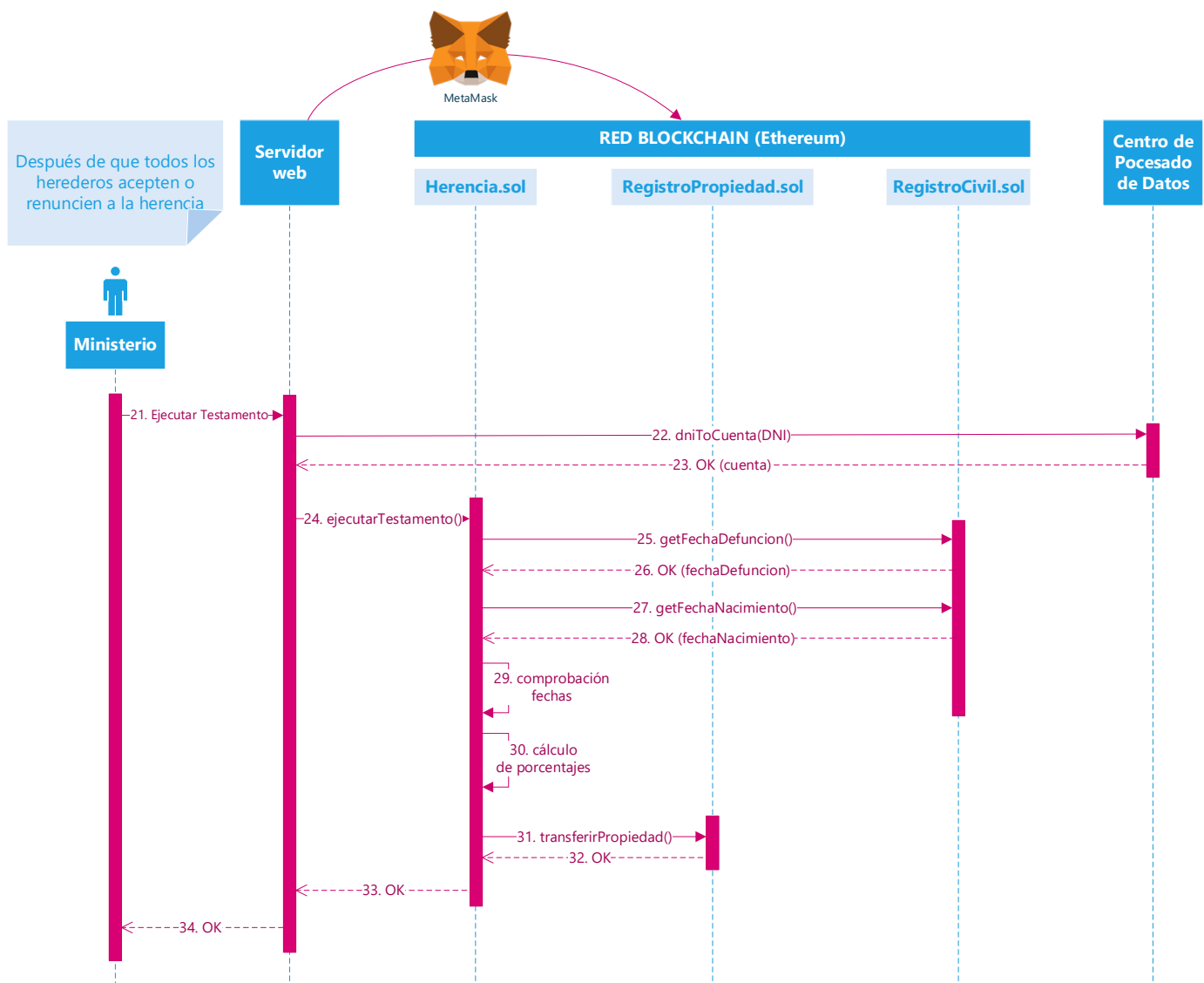


Ilustración 21. Diagrama de secuencia del proceso de herencia (II)

5.2.6 DISEÑO DEL FRONT-END

Por último, se plantea como estará estructurada la información que se muestra al usuario en el *front-end*, para ello se ha elaborado un diseño esquemático de las pantallas a través de las cuales los usuarios interactuarán con la aplicación.

La aplicación constará de dos pantallas, una para cada tipo de usuario, que se programarán usando el paradigma de las webs dinámicas⁴ en vez de crear una web estática con navegación entre múltiples pantallas fijas. Esto facilitará la usabilidad a los clientes y permitirá que la interacción con la aplicación sea más intuitiva.

La primera de las pantallas será para el usuario Ministerio, encargado de administrar el Registro Civil, Registro de la Propiedad y ejecutar testamentos. A continuación, en la *Ilustración 22* se muestra un diagrama estructural de la información que se mostrará en dicha pantalla.

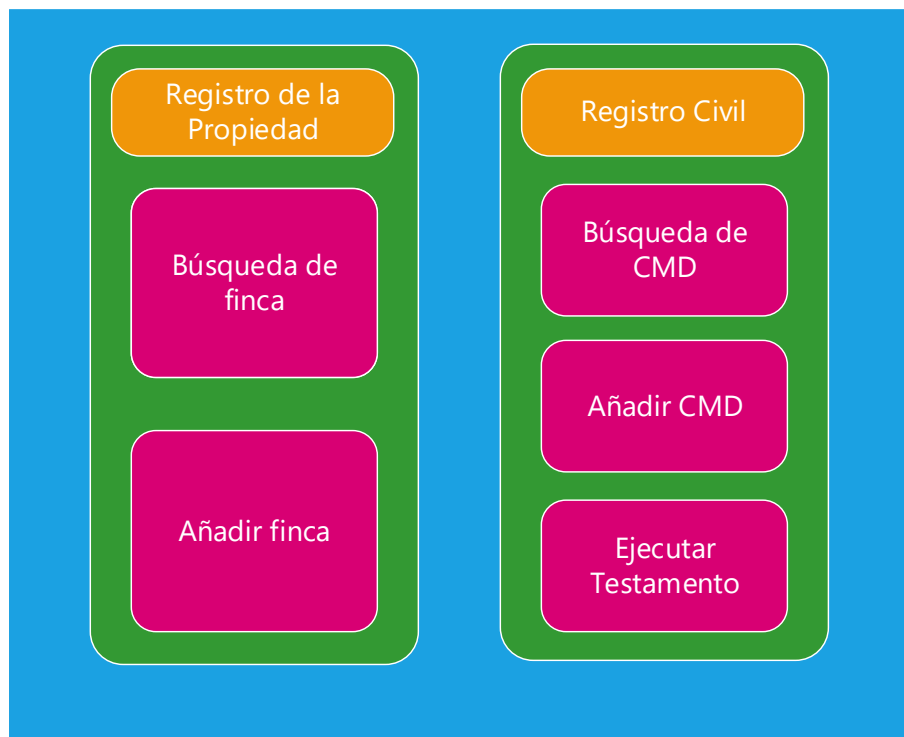


Ilustración 22. Diagrama estructural de la pantalla del usuario Ministerio

La segunda de las pantallas será para el usuario Cliente, en ella los clientes en condición de testador podrán elaborar testamentos y consultar sus Certificados de Últimas Voluntades

⁴ **Webs dinámicas:** Hace referencia a aquellas páginas webs con contenido se genera de forma automática cuando el usuario solicita su visualización. Van cambiando dinámicamente sin la necesidad de navegar entre pantallas estáticas.

mientras que los clientes en condición de herederos podrán consultar los trámites pendientes y aceptar o renunciar a las herencias en las que se les han nombrado herederos. En la *Ilustración 23* se muestra un diagrama estructural de la información que se mostrará en dicha pantalla.



Ilustración 23. Diagrama estructural de la pantalla del usuario Cliente

5.3 IMPLEMENTACIÓN

Una vez presentado el diseño del modelo, se procede a su desarrollo e implantación de la aplicación. En la *Ilustración 24*, se presenta un diagrama de flujo de la evolución del desarrollo e implantación del proyecto.

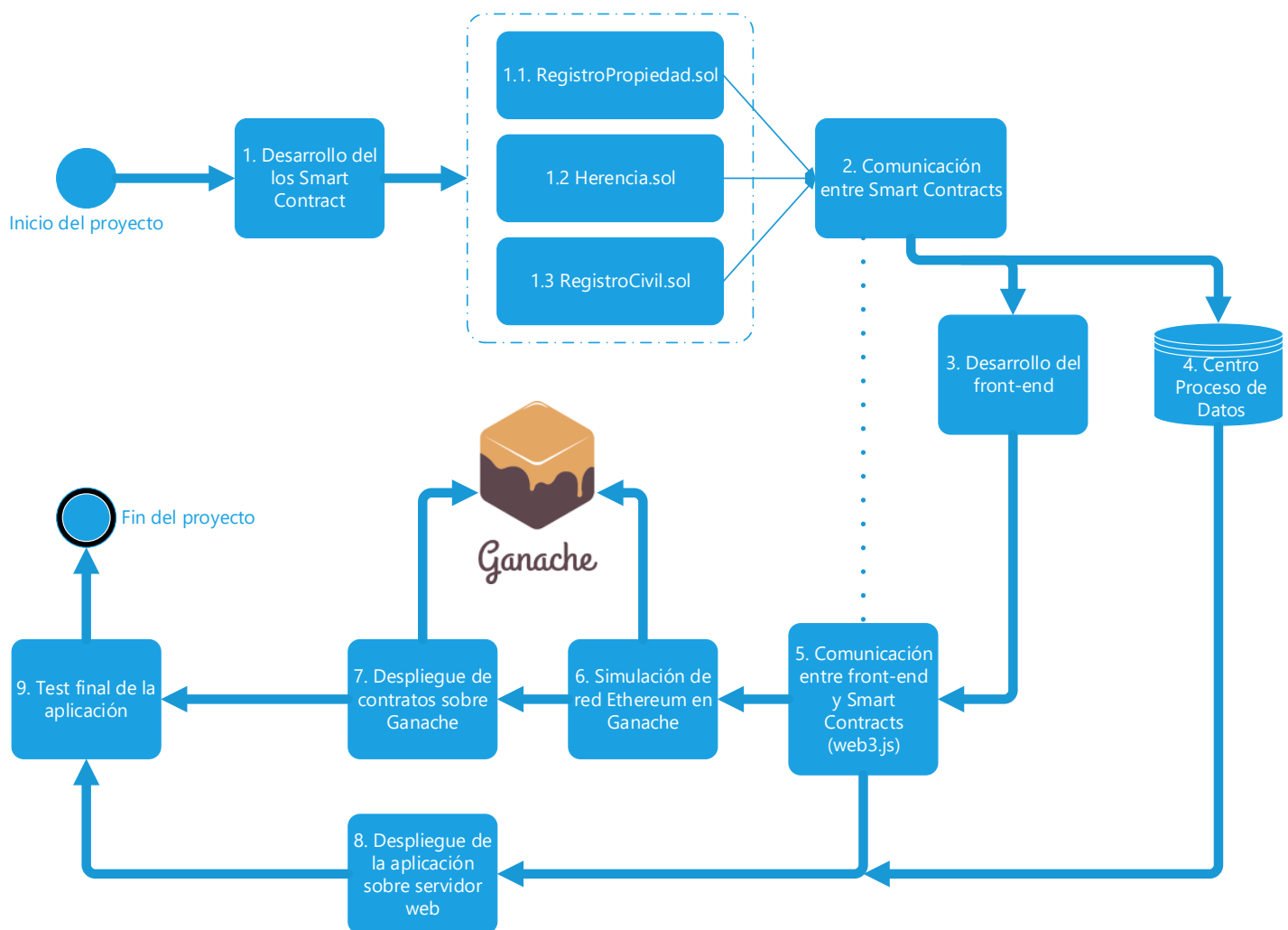


Ilustración 24. Diagrama de flujo del proceso de desarrollo de la aplicación web

Para ello en primer lugar se realiza el desarrollo del *back-end*, es decir, se programan los tres Smart Contract (1), RegistroPropiedad.sol, RegistroCivil.sol y Herencia.sol tal y como especifica el diseño en el apartado 5.2. Esta tarea se ha realizado en el IDE Remix, el cual a

medida que se iba realizando el desarrollo de los contratos, podían desplegarse sobre un emulador basado en JavaScript y comprobar su funcionamiento.

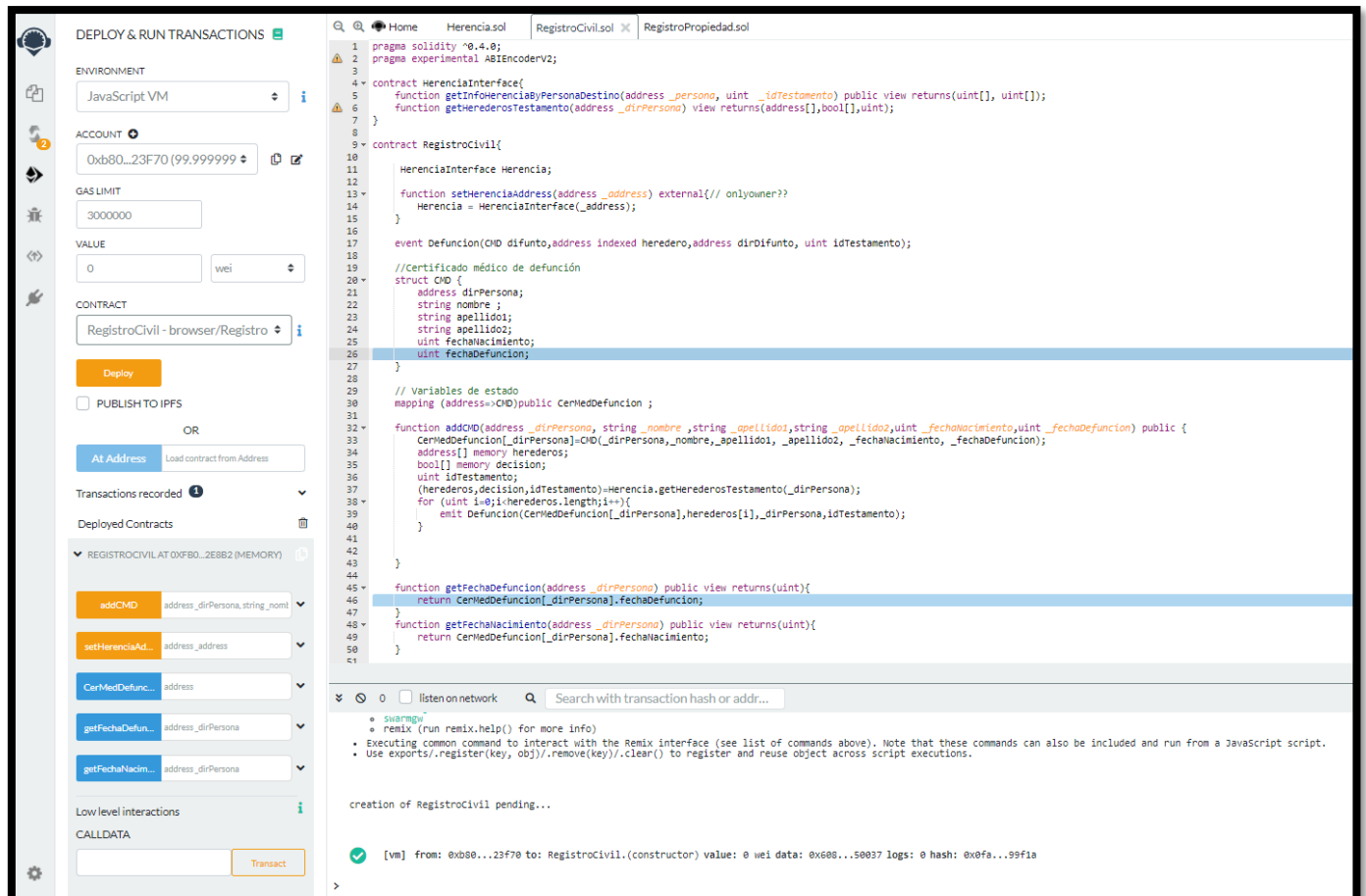


Ilustración 25. Captura de IDE Remix en el proceso de desarrollo

A continuación, una vez terminado cada uno de los contratos, se crean las interfaces que permiten la comunicación entre los contratos (2) y ejecutar métodos de otros contratos distintos. Esto permite que la lógica de Herencia.sol pueda directamente transferir propiedades con métodos de RegistroPropiedad.sol y consultar propiedades en la cadena de bloques de dicho contrato sin la necesidad de un intermediario. Esto es una ventaja que añade mayor seguridad al proceso de herencia ya que si se añadiera para esta tarea un intermediario como un servidor o persona humana, el proceso de herencia y transferencia de propiedades dependería del control por parte de un elemento ajeno a la red descentralizada por lo que dejaría de garantizarse la confiabilidad y seguridad que otorga la red en el proceso.

Una vez que funciona correctamente cada contrato por separado y la comunicación entre ellos, se procede al desarrollo del *front-end* (3) mediante los lenguajes de programación HTML, CSS y JavaScript.

En paralelo, se desarrolla la base de datos (4) que simula el Centro de Proceso de Datos y que contiene los Documentos Nacionales de Identidad vinculados a las respectivas cuentas de la red Ethereum de cada ciudadano. La base de datos podrá administrarse por línea de comandos o mediante un administrador de base de datos, phpMyAdmin como se muestra en la *Ilustración 26*.

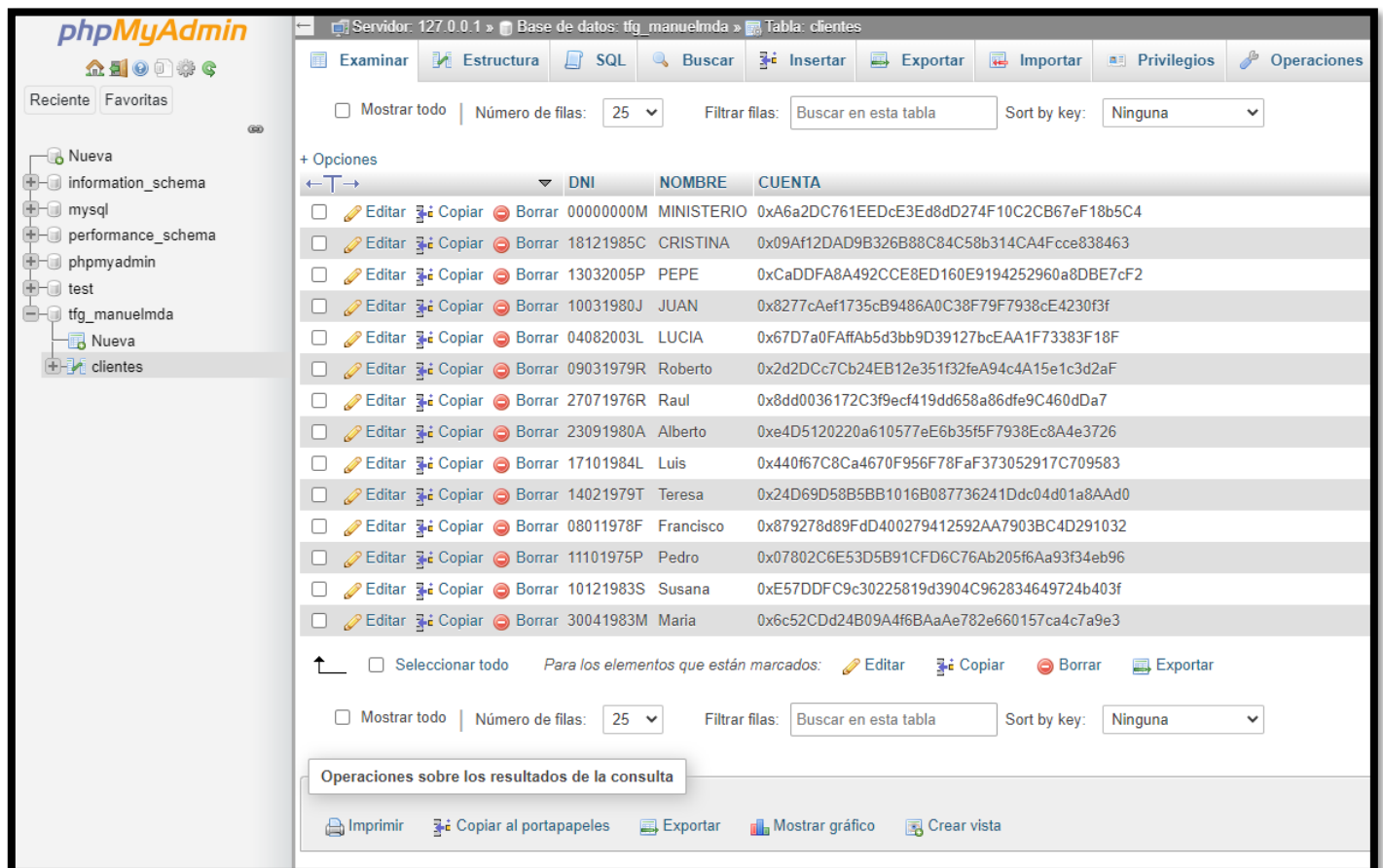
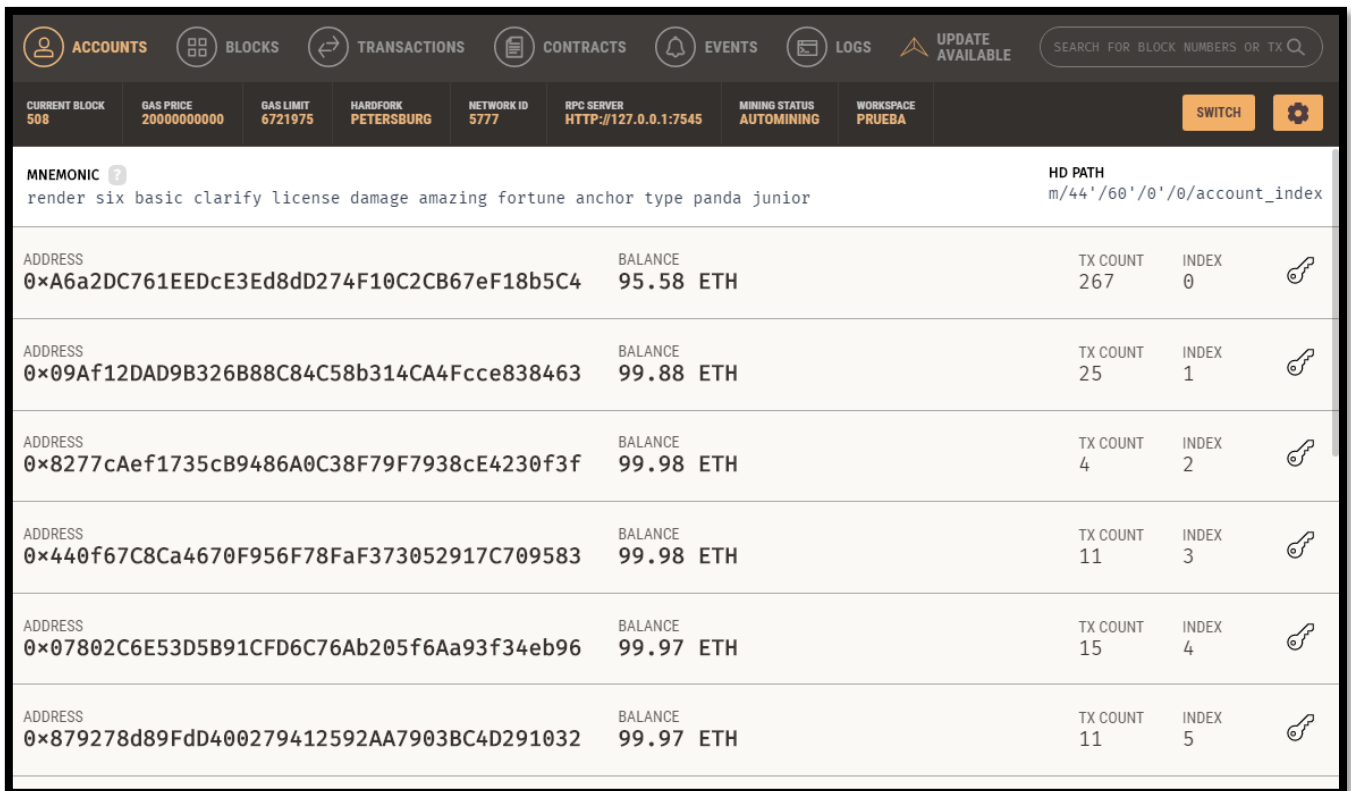


Ilustración 26. Captura del administrador de base de datos phpMyAdmin durante el desarrollo

Una vez que el *front-end* está listo, se establece comunicación entre el *front-end* y la base de datos (5) mediante consultas SQL a través de un script en PHP que permite obtener los valores de las cuentas a partir de los DNIs y viceversa.

También se establece comunicación entre el *frond-end* y el *back-end* mediante web3.js (5), que permite ejecutar los métodos del *back-end* y resolver las solicitudes mediante *promises*.

Cuando está todo el desarrollo terminado, se procede a la simulación de la red de blockchain Ethereum en Ganache (6), programa que permite simular redes Ethereum con sus nodos y desplegar Smart Contracts para probar su correcto funcionamiento (Ver *Ilustración 27*). En este proyecto será aquí donde se probará la aplicación pues debido a la legislación vigente en España y casuística del proyecto, no se puede desplegar en la red real de Ethereum.



The screenshot shows the Ganache interface with the following components:

- Top Navigation Bar:** ACCOUNTS, BLOCKS, TRANSACTIONS, CONTRACTS, EVENTS, LOGS, UPDATE AVAILABLE.
- Search Bar:** SEARCH FOR BLOCK NUMBERS OR TX
- Account Information:**
 - CURRENT BLOCK: 508
 - GAS PRICE: 20000000000
 - GAS LIMIT: 6721975
 - HARDFORK: PETERSBURG
 - NETWORK ID: 5777
 - RPC SERVER: HTTP://127.0.0.1:7545
 - MINING STATUS: AUTOMINING
 - WORKSPACE: PRUEBA
 - Buttons: SWITCH, Settings
- MNEMONIC:** render six basic clarify license damage amazing fortune anchor type panda junior
- HD PATH:** m/44'/60'/0'/0/account_index
- Accounts Table:**

ADDRESS	BALANCE	TX COUNT	INDEX	
0xA6a2DC761EEDcE3Ed8dD274F10C2CB67eF18b5C4	95.58 ETH	267	0	
0x09Af12DAD9B326B88C84C58b314CA4Fcce838463	99.88 ETH	25	1	
0x8277cAef1735cB9486A0C38F79F7938cE4230f3f	99.98 ETH	4	2	
0x440f67C8Ca4670F956F78FaF373052917C709583	99.98 ETH	11	3	
0x07802C6E53D5B91CFD6C76Ab205f6Aa93f34eb96	99.97 ETH	15	4	
0x879278d89FdD400279412592AA7903BC4D291032	99.97 ETH	11	5	

Ilustración 27. Captura de Ganache simulando una red descentralizada durante el desarrollo

Posteriormente se desplegarán los contratos sobre la red simulada (7) y se desplegará la aplicación desarrollada sobre el servidor web (8).

Para finalizar, se realizan las pruebas necesarias y comprobación final de la aplicación (9), que, en caso de obtener resultados satisfactorios, se dará por terminado el desarrollo del proyecto.

Capítulo 6. ANÁLISIS DE RESULTADOS

Tras el desarrollo del proyecto, se ha conseguido llegar a buen término con los objetivos de diseño marcados en el Capítulo 5.

Cabe destacar que el proyecto se ha centrado en demostrar que existe la tecnología necesaria para establecer un nuevo modelo capaz de sustituir al tradicional en los procesos de elaboración de testamentos y del proceso de herencia, por lo tanto, se ha buscado conseguir un modelo funcional siguiendo el diseño mencionado *Capítulo 5*. con un correcto funcionamiento de las tecnologías y no ha estado centrado tanto en conseguir una apariencia visual llamativa para el cliente.

Como se pudo ver en *Ilustración 24. Diagrama de flujo del proceso de desarrollo de la aplicación web*, los primeros pasos del desarrollo de la aplicación web consistían en el desarrollo del *back-end* con la programación de los Smart Contract y comunicación entre ellos a través de las interfaces.

Durante esta parte, se han ido haciendo pruebas unitarias de las funcionalidades que los contratos iban incorporando y una vez que los contratos estaban terminados, se procedía a realizar pruebas de integración entre ellos. En caso de fallo de algún método o funcionalidad de los contratos, se procedía a su corrección, en ocasiones con el debugger de transacciones que incluye IDE Remix, y posteriormente se realizaban pruebas de regresión para comprobar su correcto funcionamiento sin que hubiera interferencias con el funcionamiento del resto de módulos.

Para comprobar su funcionamiento, los contratos son desplegados sobre una red Ethereum simulada en una aplicación llamada Ganache. Durante este paso, se comprueba que los contratos quedan desplegados sobre esta red correctamente y se realizan pruebas de integración comprobando que los tres contratos programados no solo funcionan de forma independiente, sino también en conjunto. Para ello, primero se despliegan los tres contratos,

quedando cada uno identificado con una dirección que permitirá acceder a ellos desde el *front-end* o desde otros contratos para integrarlos en otras aplicaciones.

En la *Ilustración 28*, se muestra una captura durante el proceso de despliegue de los contratos sobre la red de blockchain. En el círculo verde de dicha imagen, se pueden ver los contratos desplegados en la red, mientras que, en el círculo azul, las transacciones que se van realizando en la red. Cada una de las transacciones que se muestran en la imagen corresponden al despliegue de un contrato o configuración de la comunicación mediante las interfaces, y como se muestra al lado de cada una, todas las transacciones han sido satisfactorias.

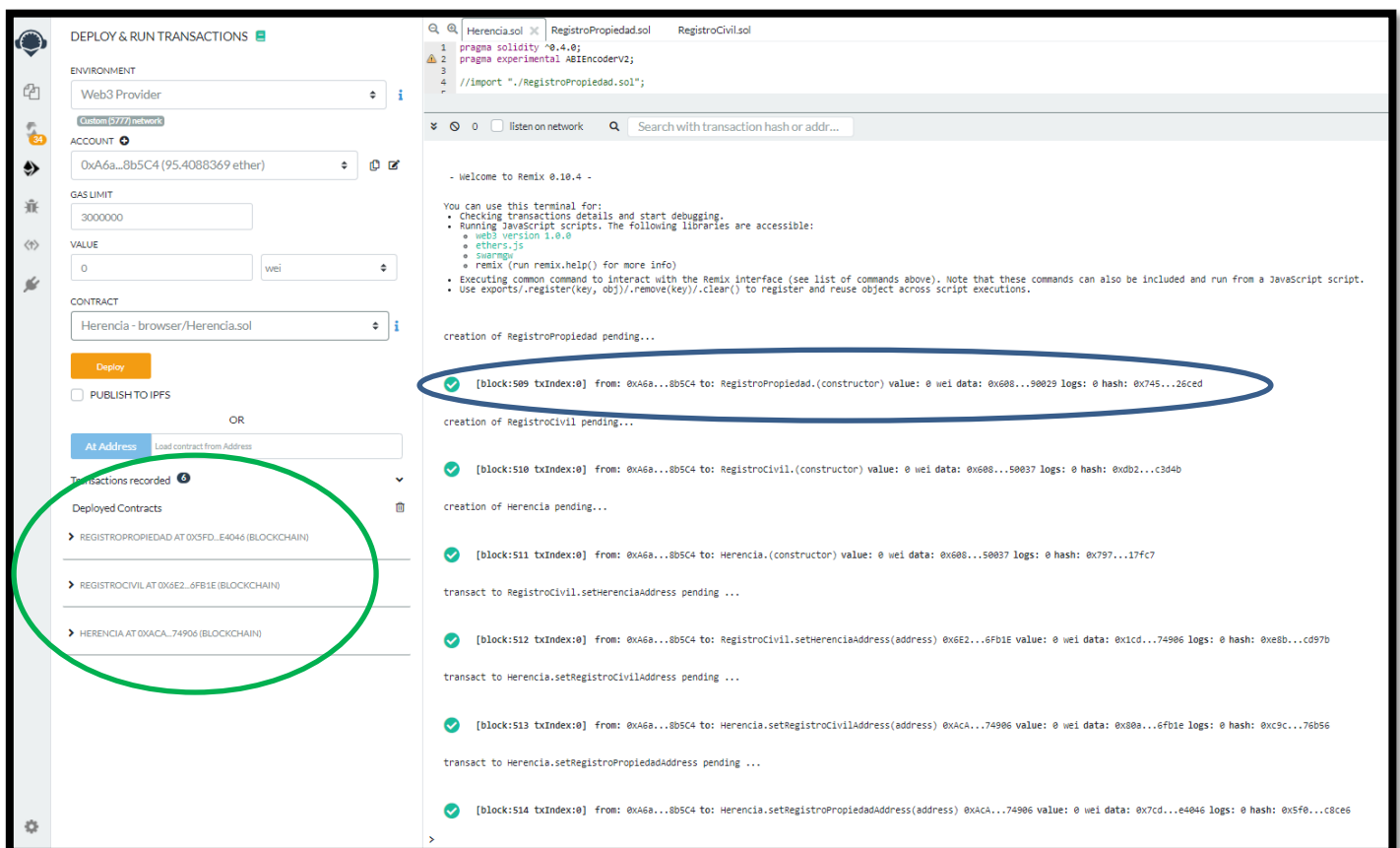
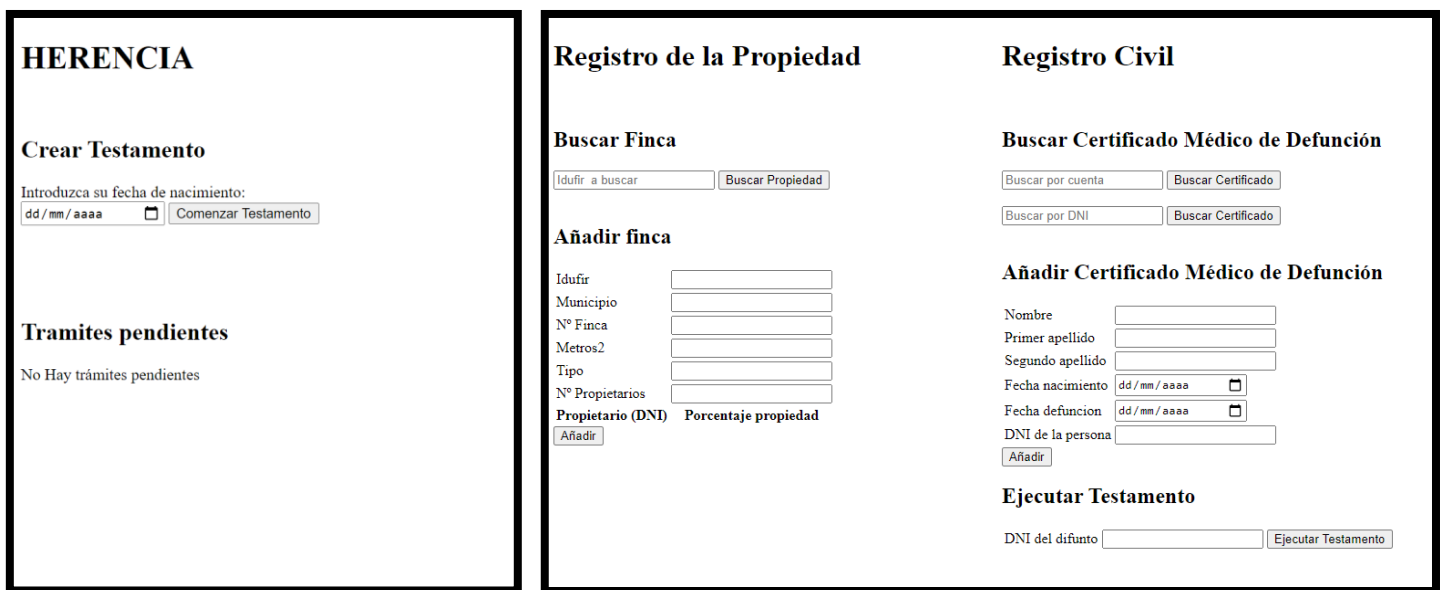


Ilustración 28. Captura durante despliegue de contratos y pruebas de integración

Durante el siguiente paso, el desarrollo del *front-end* los resultados pueden verse directamente en un navegador web, ya que HTML es un lenguaje compilado *Just in Time* o

interpretado por lo que no requiere de un compilado para ver los resultados durante el desarrollo.

A continuación, se muestra en la *Ilustración 29*, el resultado del *front-end* para los actores Clientes y Ministerio. Al no estar la página conectada todavía al *back-end*, no se muestra ninguna información, pero más adelante, cuando se conecte el *back-end* con el *front-end* se podrá visualizar la información de los clientes que se conecten a la aplicación.



The screenshot displays three distinct user interface sections for a legal application:

- HERENCIA (Inheritance):** Contains a 'Crear Testamento' (Create Will) section with a date input field and a 'Comenzar Testamento' button. Below it, a 'Tramites pendientes' (Pending procedures) section shows the message 'No Hay trámites pendientes'.
- Registro de la Propiedad (Property Registry):** Includes a 'Buscar Finca' (Search Property) section with an 'Idufir a buscar' input and a 'Buscar Propiedad' button. Below this is an 'Añadir finca' (Add property) section with multiple input fields for 'Idufir', 'Municipio', 'Nº Finca', 'Metros2', 'Tipo', 'Nº Propietarios', 'Propietario (DNI)', and 'Porcentaje propiedad', along with an 'Añadir' button.
- Registro Civil (Civil Registry):** Features a 'Buscar Certificado Médico de Defunción' (Search Medical Death Certificate) section with inputs for 'Buscar por cuenta' and 'Buscar por DNI', each with a 'Buscar Certificado' button. Below is an 'Añadir Certificado Médico de Defunción' section with inputs for 'Nombre', 'Primer apellido', 'Segundo apellido', 'Fecha nacimiento', 'Fecha defuncion', and 'DNI de la persona', each with a corresponding 'Añadir' button. At the bottom, an 'Ejecutar Testamento' (Execute Will) section includes a 'DNI del difunto' input and an 'Ejecutar Testamento' button.

Ilustración 29. Capturas del front-end de la aplicación durante el desarrollo

Al mismo tiempo, se configuró la base de datos que simula el Centro de Proceso de Datos. Se trata de una base de datos *SQL* que puede administrarse por línea de comandos o desde el administrador *phpMyAdmin*. A continuación, en la *Ilustración 30* se muestra una captura de varias consultas realizadas a la base de datos por línea de comandos.

```
mysql> select DNI, NOMBRE, CUENTA from CLIENTES;
```

DNI	NOMBRE	CUENTA
0000000M	MINISTERIO	0xA6a2DC761EEDcE3Ed8dD274F10C2C867eF18b5C4
18121985C	CRISTINA	0x09Af12DAD9B326B88C84C58b314CA4Fcce838463
10031980J	JUAN	0x8277cAef1735cB9486A0C38F79F7938cE4230f3F
04082003L	LUCIA	0x6707a0FAffab5d3bb0D39127bcEAA1F73383F18F
13032005P	PEPE	0xCaDDFA8A492CCE8ED160E9194252960a8D8E7cF2
17101984L	Luis	0x440f67C8Ca4670F956F78FaF373052917C709583
11101975P	Pedro	0x07802C6E53D5891CFD6C76Ab205f6Aa93f34eb96
08011978F	Francisco	0x879278d89Fd0400279412592AA7903BC4D291032
10121983S	Susana	0xE57DDFC9c30225819d3904C962834649724b403f
09031979R	Roberto	0x2d2DCc7Cb24EB12e351f32FeA94c4A15e1c3d2aF
23091980A	Alberto	0xe4D5120220a610577eE6b35f5F7938Ec8A4e3726
27071976R	Raul	0x8dd0036172C3f9ecf419dd658a86dfe9C460d0a7
30041983M	Maria	0x6c52CDd24809A4f6BAaAe782e660157ca4c7a9e3
14021979T	Teresa	0x24069D58858B10168087736241Ddc04d01aAAAd0

```
14 rows in set (0.00 sec)
```

```
mysql> select CUENTA from CLIENTES where DNI='18121985C';
```

CUENTA
0x09Af12DAD9B326B88C84C58b314CA4Fcce838463

```
1 row in set (0.00 sec)
```

```
mysql> select NOMBRE, CUENTA from CLIENTES where DNI='18121985C';
```

NOMBRE	CUENTA
CRISTINA	0x09Af12DAD9B326B88C84C58b314CA4Fcce838463

```
1 row in set (0.00 sec)
```

Ilustración 30. Consultas de datos realizadas por línea de comandos con sentencias SQL

Por último, antes de proceder al realizar el testeo final de la aplicación, se realizan pruebas de encadenamiento entre el *front-end* y el *back-end* para comprobar que la comunicación entre ambas es satisfactoria. Estas pruebas se realizan por consola desde el navegador web, aunque también pueden realizarse desde la línea de comandos de un ordenador.

Tanto cuando se solicita datos como cuando se modifica el estado de la red de blockchain, estas operaciones se realizan mediante la invocación de *promises* (promesas), las cuales se tratan de un objeto que representa una operación asíncrona terminada de forma satisfactoria o fracasada. A continuación, se muestra en *Ilustración 31* e *Ilustración 32* dos *promises* solicitando a la red de blockchain la información de un Certificado Médico de Defunción (CMD) registrado en el contrato desplegado del Registro Civil un CMD y la información de una finca registrada en el contrato desplegado del Registro de la Propiedad. Al ser satisfactoria la resolución de la *promise*, el *back-end* devuelve una estructura de datos con la información solicitada.

```
> var cmd
< undefined
> var cuentaBusqueda= "0x09Af12DAD9B326888C84C58b314CA4Fcce838463"
< undefined
> ContratoRegistroCivil.methods.CerMedDefuncion(cuentaBusqueda).call((err,result)=>{cmd=result})
< Promise {<pending>}
  __proto__: Promise
  [[PromiseStatus]]: "fulfilled"
  [[PromiseValue]]: d
> cmd
< d {0: "0x09Af12DAD9B326888C84C58b314CA4Fcce838463", 1: "Cristina", 2: "gomez", 3: "perez", 4: "503712000", 5: "1595376000", dirPersona:
  0x09Af12DAD9B326888C84C58b314CA4Fcce838463", nombre: "Cristina", apellido1: "gomez", apellido2: "perez", fechaNacimiento: "50371200
0", ...}
  0: "0x09Af12DAD9B326888C84C58b314CA4Fcce838463"
  1: "Cristina"
  2: "gomez"
  3: "perez"
  4: "503712000"
  5: "1595376000"
  apellido1: "gomez"
  apellido2: "perez"
  dirPersona: "0x09Af12DAD9B326888C84C58b314CA4Fcce838463"
  fechaDefuncion: "1595376000"
  fechaNacimiento: "503712000"
  nombre: "Cristina"
  __proto__: Object
```

Ilustración 31. Resolución de una promesa solicitando un CMD a la red de blockchain

```
> var finca
< undefined
> var id="1111"
< undefined
> ContratoRegistroPropiedad.methods.getPropiedad(id).call((err,result)=>{finca=result})
< Promise {<pending>}
> finca
< d {0: "1111", 1: "Madrid", 2: "23", 3: "245", 4: "Chalet", 5: Array(2), 6: Array(2)}
  0: "1111"
  1: "Madrid"
  2: "23"
  3: "245"
  4: "Chalet"
  5: (2) ["0x67D7a0FAffAb5d3bb9D39127bcEAA1F73383F18F", "0xCaDDFA8A492CCE8ED160E9194252960a8D8E7cF2"]
  6: (2) ["50", "50"]
  __proto__: Object
```

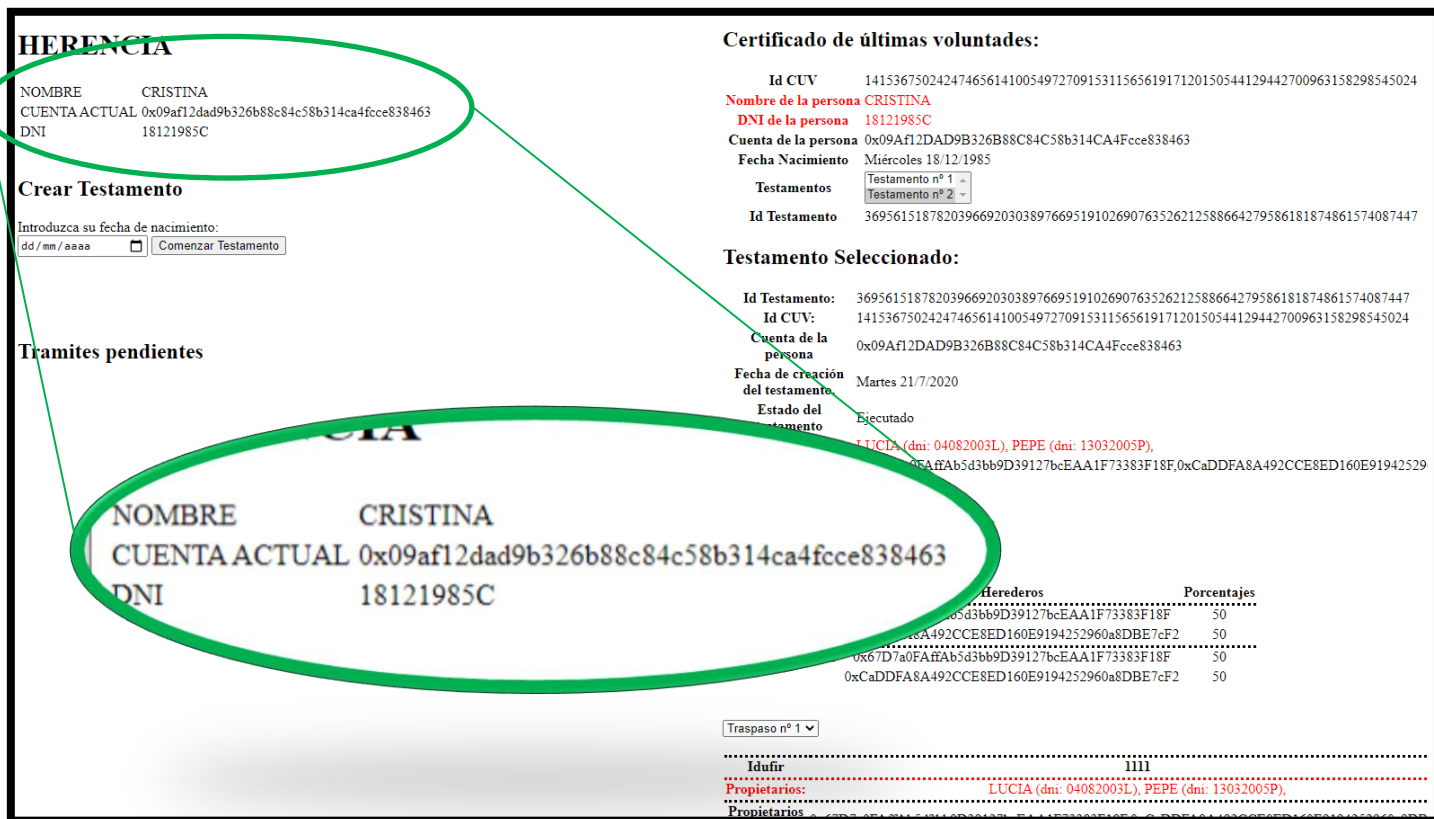
Ilustración 32. Resolución de una promesa solicitando información de una finca a la red de blockchain

Finalmente, una vez que funcionan todos los componentes del proyecto, se procede a comprobar en conjunto que la integración y encadenamiento de todos los módulos de la aplicación funcionan correctamente y la usabilidad del producto es válida.

A continuación, se muestran unas imágenes del resultado del proyecto; para más detalles del uso de la aplicación, consúltese

Anexo III: Manual del usuario que contiene el manual de usuario con las instrucciones del uso de la aplicación.

En primer lugar, tal y como se aprecia en la parte superior izquierda de las pantallas del Ministerio y del Cliente se muestra la información del usuario correspondiente a la cuenta activa en MetaMask. Véase *Ilustración 33* a continuación.



HERENCIA

NOMBRE CRISTINA
CUENTA ACTUAL 0x09af12dad9b326b88c84c58b314ca4fccc838463
DNI 18121985C

Crear Testamento

Introduzca su fecha de nacimiento:
dd/mm/aaaa ☐ Comenzar Testamento

Tramites pendientes

NOMBRE CRISTINA
CUENTA ACTUAL 0x09af12dad9b326b88c84c58b314ca4fccc838463
DNI 18121985C

Certificado de últimas voluntades:

Id CUV 14153675024247465614100549727091531156561917120150544129442700963158298545024
Nombre de la persona CRISTINA
DNI de la persona 18121985C
Cuenta de la persona 0x09Af12DAD9B326B88C84C58b314CA4Fccc838463
Fecha Nacimiento Miércoles 18/12/1985
Testamentos Testamento nº 1
Id Testamento 36956151878203966920303897669519102690763526212588664279586181874861574087447

Testamento Seleccionado:

Id Testamento: 36956151878203966920303897669519102690763526212588664279586181874861574087447
Id CUV: 14153675024247465614100549727091531156561917120150544129442700963158298545024
Cuenta de la persona 0x09Af12DAD9B326B88C84C58b314CA4Fccc838463
Fecha de creación del testamento Martes 21/7/2020
Estado del testamento Ejecutado
Idioma LUCIA (dni: 04082003L), PEPE (dni: 13032005P),
0x67D7a0FAfAb5d3bb9D39127bcEAA1F73383F18F, 0xCaDDFA8A492CCE8ED160E91942529

Herederos	Porcentajes
0x67D7a0FAfAb5d3bb9D39127bcEAA1F73383F18F	50
0xCaDDFA8A492CCE8ED160E9194252960a8DBE7cF2	50
0x67D7a0FAfAb5d3bb9D39127bcEAA1F73383F18F	50
0xCaDDFA8A492CCE8ED160E9194252960a8DBE7cF2	50

Traspaso nº 1

Idioma LUCIA (dni: 04082003L), PEPE (dni: 13032005P),
Propietarios: LUCIA (dni: 04082003L), PEPE (dni: 13032005P),
Propietarios

Ilustración 33. Detalle de la información del usuario conectado a la aplicación

La pantalla de administración del Ministerio, mostrada en la *Ilustración 34* está dividida en dos partes, por un lado, en la zona izquierda se encuentra todo lo referente al Registro de la Propiedad y por otro, en la zona derecha se encuentra lo referente al Registro Civil.

Registro de la Propiedad

NOMBRE MINISTERIO
CUENTA ACTUAL 0xa6a2dc761eedce3ed8dd274f10c2cb67ef18b5c4
DNI 0000000M

Buscar Finca

Idufir a buscar

Añadir finca

Idufir
Municipio
Nº Finca
Metros2
Tipo
Nº Propietarios
Propietario (DNI) Porcentaje propiedad

Registro Civil

Buscar Certificado Médico de Defunción

Añadir Certificado Médico de Defunción

Nombre
Primer apellido
Segundo apellido
Fecha nacimiento
Fecha defuncion
DNI de la persona

Ejecutar Testamento

DNI del difunto

Ilustración 34. Captura de la vista del usuario Ministerio

En cuanto al resultado de la parte de la aplicación que corresponde con el Registro de la Propiedad puede verse un ejemplo de la administración de este registro en la *Ilustración 36*. En la parte de la izquierda de dicha imagen, se muestra el proceso de registro de una finca y en la derecha la consulta de una propiedad a partir del Idufir.

Por otro lado, en cuanto al resultado de la zona de Registro Civil, en la *Ilustración 35* puede verse un ejemplo de la administración en este registro. Por un lado, en la zona izquierda se puede ver el proceso de registro de un Certificado Médico de Defunción CMD y en la parte derecha la consulta realizada de un certificado a partir del Documento Nacional de Identidad o de la cuenta Ethereum de una persona.

Registro de la Propiedad

NOMBRE MINISTERIO
CUENTA ACTUAL 0xa6a2dc761eedce3ed8dd274f10c2cb67ef18b5c4
DNI 00000000M

Buscar Finca

Idufir a buscar Buscar Propiedad

Añadir finca

Idufir
Municipio
Nº Finca
Metros2
Tipo
Nº Propietarios

Propietario (DNI)	Porcentaje propiedad
11101975P	40
04082003L	60

Registro de la Propiedad

NOMBRE MINISTERIO
CUENTA ACTUAL 0xa6a2dc761eedce3ed8dd274f10c2cb67ef18b5c4
DNI 00000000M

Buscar Finca

Idufir:
Municipio:
Nº Finca:
M2:
Tipo:

Propietarios	DNI	Cuentas	Porcentajes
Pedro	11101975P	0x07802C6E53D5B91CFD6C76Ab205f6Aa93f34eb96	40
LUCIA	04082003L	0x67D7a0FAfAb5d3bb9D39127bcEAA1F73383F18F	60

Añadir finca

Idufir
Municipio
Nº Finca
Metros2
Tipo
Nº Propietarios

Propietario (DNI)	Porcentaje propiedad

Ilustración 36. Administración del Registro de la Propiedad

Registro Civil

Buscar Certificado Médico de Defunción

Buscar por cuenta
Buscar por DNI

Añadir Certificado Médico de Defunción

Nombre
Primer apellido
Segundo apellido
Fecha nacimiento
Fecha defuncion
DNI de la persona

Certificado Médico de Defunción añadido para cuenta
0x09Af12DAD9B326B88C84C58b314CA4Fcce838463

Ejecutar Testamento

DNI del difunto

Registro Civil

Buscar Certificado Médico de Defunción

Buscar por cuenta

Dni:
Cuenta:
Nombre:
1º Apellido:
2º Apellido:
Fecha de nacimiento:
Fecha de defuncion:

Añadir Certificado Médico de Defunción

Nombre
Primer apellido
Segundo apellido
Fecha nacimiento
Fecha defuncion
DNI de la persona

Ejecutar Testamento

DNI del difunto

Ilustración 35. Administración del Registro Civil

La pantalla del usuario cliente, mostrada en la Ilustración 37 está dividida en dos partes, por un lado, la parte izquierda donde el cliente podrá realizar las gestiones oportunas en cuanto a los testamentos y por otro lado la parte derecha dedicada a la visualización de los datos del cliente.

HERENCIA

NOMBRE CRISTINA
CUENTA ACTUAL 0x09af12dad9b326b88c84c58b314ca4fccc838463
DNI 18121985C

Crear Testamento

Introduzca su fecha de nacimiento:
dd/mm/aaaa

Tramites pendientes

Certificado de Últimas Voluntades:

Id CUV 14153675024247465614100549727091531156561917120150544129442700963158298545024
Nombre de la persona CRISTINA
DNI de la persona 18121985C
Cuenta de la persona 0x09Af12DAD9B326B88C84C58b314CA4Fccc838463
Fecha Nacimiento Miércoles 18/12/1985
Testamentos
Id Testamento 36956151878203966920303897669519102690763526212588664279586181874861574087447

Testamento seleccionado:

Id Testamento: 36956151878203966920303897669519102690763526212588664279586181874861574087447
Id CUV: 14153675024247465614100549727091531156561917120150544129442700963158298545024
Cuenta de la persona 0x09Af12DAD9B326B88C84C58b314CA4Fccc838463
Fecha de creación del testamento. Martes 21/7/2020
Estado del testamento Ejecutado
Herederos LUCIA (dni: 04082003L), PEPE (dni: 13032005P),
Cuentas herederos 0x67D7a0FAffAb5d3bb9D39127bcEAA1F73383F18F,0xCaDDFA8A492CCE8ED160E9194252960a8DBE7cF2
Decisión de herederos(true/false) true,true

Resumen Traspasos

Nº Traspaso	Idufir	Herederos	Porcentajes
1	2222	0x67D7a0FAffAb5d3bb9D39127bcEAA1F73383F18F	50
		0xCaDDFA8A492CCE8ED160E9194252960a8DBE7cF2	50
2	1111	0x67D7a0FAffAb5d3bb9D39127bcEAA1F73383F18F	50
		0xCaDDFA8A492CCE8ED160E9194252960a8DBE7cF2	50

Traspaso nº 2

Idufir	Propietarios	Propietarios (Cuentas)	Propietarios
2222	LUCIA (dni: 04082003L), PEPE (dni: 13032005P),	0x67D7a0FAffAb5d3bb9D39127bcEAA1F73383F18F,0xCaDDFA8A492CCE8ED160E9194252960a8DBE7cF2	50,50

Ilustración 37. Captura de la vista del usuario Cliente

A continuación, en la Ilustración 38 se muestran varias capturas de las operaciones que puede realizar el cliente. En la zona superior de dicha ilustración, se muestra el proceso de escritura de testamento por parte de un testador mientras que abajo, se pueden ver los trámites pendientes de dicho cliente, en el caso particular de la captura, no hay ningún trámite pendiente pues ya ha aceptado todas las herencias en las que el cliente ha sido nombrado heredero.

Crear Testamento

Introduzca su fecha de nacimiento:

04/08/2003

Testamento creado con id:48834789057082941996896641129577991131555208344504225419620381359069361479574

9999

Sevilla Apartamento Porcentaje: 100

Introduzca numero de herederos:

-Propietario (dni) 1 Porcentaje

-Propietario (dni) 2 Porcentaje

1111

Madrid Chalet Porcentaje: 50

Introduzca numero de herederos:

-Propietario (dni) 1 Porcentaje

2222

Madrid Plaza garaje Porcentaje: 30

Introduzca numero de herederos:

-Propietario (dni) 1 Porcentaje

-Propietario (dni) 2 Porcentaje

4553

Madrid Piso Porcentaje: 60

Introduzca numero de herederos:

-Propietario (dni) 1 Porcentaje

Tramites pendientes

Usuario fallecido: CRISTINA (DNI: 18121985C)

Cuenta del usuario: 0x09Af12DAD9B326B88C84C58b314CA4Fcce838463

Id testamento: 36956151878203966920303897669519102690763526212588664279586181874861574087447

Aceptado

Usuario fallecido: JUAN (DNI: 10031980J)

Cuenta del usuario: 0x8277cAef1735cB9486A0C38F79F7938cE4230f3f

Id testamento: 75735203776523051016006900687072266762885385792437754270261715912992950666770

Aceptado

Ilustración 38. Proceso de escritura de Testamento (Superior), Trámites pendientes (Inferior)

Finalmente, en la *Ilustración 39* se muestra toda la información que el usuario puede visualizar, al acceder a la aplicación web, sobre su Certificado de Últimas Voluntades y los detalles que desee como consultar en mayor profundidad los testamentos realizados. Esta información se carga automáticamente al detectar el usuario conectado en ese momento.

Certificado de Últimas Voluntades:

Id CUV 52071488529374516351802143686454834689784304583090914601038826925917018002478
Nombre de la persona LUCIA
DNI de la persona 04082003L
Cuenta de la persona 0x67D7a0FAffAb5d3bb9D39127bcEAA1F73383F18F
Fecha Nacimiento Lunes 4/8/2003
Testamentos Testamento nº 1
Id Testamento 48834789057082941996896641129577991131555208344504225419620381359069361479574

Testamento seleccionado:

Id Testamento: 48834789057082941996896641129577991131555208344504225419620381359069361479574
Id CUV: 52071488529374516351802143686454834689784304583090914601038826925917018002478
Cuenta de la persona 0x67D7a0FAffAb5d3bb9D39127bcEAA1F73383F18F
Fecha de creación del testamento. Domingo 16/8/2020
Estado del testamento Sin Ejecutar
Herederos Maria (dni: 30041983M), Teresa (dni: 14021979T),
Cuentas herederos 0x6c52CDd24B09A4f6BAaAe782e660157ca4c7a9e3,0x24D69D58B5BB1016B087736241Ddc04d01a8AAAd0
Decisión de herederos(true/false) false,false

Resumen Traspasos

Nº Traspaso	Idufir	Herederos	Porcentajes
1	1111	0x6c52CDd24B09A4f6BAaAe782e660157ca4c7a9e3	100
2	9999	0x6c52CDd24B09A4f6BAaAe782e660157ca4c7a9e3	50
		0x24D69D58B5BB1016B087736241Ddc04d01a8AAAd0	50
3	2222	0x6c52CDd24B09A4f6BAaAe782e660157ca4c7a9e3	60
		0x24D69D58B5BB1016B087736241Ddc04d01a8AAAd0	40
4	4553	0x24D69D58B5BB1016B087736241Ddc04d01a8AAAd0	100

Traspaso nº 3

Idufir:	2222
Propietarios:	Maria (dni: 30041983M), Teresa (dni: 14021979T),
Propietarios (Cuentas):	0x6c52CDd24B09A4f6BAaAe782e660157ca4c7a9e3,0x24D69D58B5BB1016B087736241Ddc04d01a8AAAd0
Porcentajes	60,40
Propietarios rechazan:	
Propietarios rechazan (Cuentas)	
Porcentajes rechazan	
Propietarios aceptados:	
Propietarios aceptados (Cuentas)	
Porcentajes aceptados	

Ilustración 39. Vista de los datos mostrados del CUV de un cliente

Capítulo 7. CONCLUSIONES Y TRABAJOS FUTUROS

Este Trabajo Fin de Grado ha conseguido abordar los objetivos del proyecto marcados en el apartado 4.2 *Objetivos*.

- En primer lugar, se ha conseguido el desarrollo de una aplicación web descentralizada donde los usuarios puedan confeccionar sus testamentos con el fin de que cuando fallezcan puedan ejecutarse dichos testamentos sin seguir el modelo tradicional analizado en el apartado 5.1.
- Se ha conseguido integrar las tecnologías de Blockchain y Smart Contract otorgando transparencia y confiabilidad en todo el proceso, permitiendo la ejecución de la herencia de forma automática sin necesidad de mediadores como el notario y reduciendo la cantidad de trámites a realizar.
- Finalmente se ha podido simular una red descentralizada donde se ha desplegado la aplicación desarrollada y se ha validado su correcto funcionamiento.

Este trabajo ha conseguido demostrar que el modelo tradicional de sucesiones y herencias puede sustituirse por un modelo digital, basado en la seguridad que hoy en día aportan las tecnologías como Blockchain y Smart Contracts, sustituyendo la confiabilidad que se deposita en intermediarios durante el proceso como el notario o asesores legales.

A día de hoy, todavía se siguen realizando multitud de gestiones administrativas y jurídicas de igual forma y con los mismos modelos de hace un siglo o más tiempo como la compra de inmuebles, trazabilidad de seguros, economía y banca, o en el caso de este trabajo, las sucesiones y herencias. Esto es así pues hasta ahora no ha sido posible avanzar en dichos modelos debido a la falta de desarrollo en tecnologías que cubran estos aspectos, al contrario que en otros campos como en las telecomunicaciones que después de un siglo de avances, se ha sustituido el telégrafo por la mensajería instantánea o las conferencias telefónicas por video conferencias.

Después de haber realizado este proyecto, una de las conclusiones obtenidas es todavía la falta trabajo en estas tecnologías y desconfianza en ellas, mucha, por la falta de un gobierno central que pueda regular y controlar la red descentralizada, pero siempre y cuando la red sea lo suficientemente grande y una misma persona o entidad no disponga de la propiedad del 50% de la red, se estarán garantizando las características de seguridad descritas de esta tecnología.

También existe la posibilidad de utilizar redes descentralizadas por parte de los gobiernos con redes de ordenadores o equipos del propio gobierno. Las redes estarían bajo el control central de este, pero una persona sola no podría sabotear la información almacenada en la red.

Por otro lado, el campo legal de sucesiones y herencias es muy amplio, en este proyecto solo se ha aplicado el proceso en herencias en aquellas que solo están involucrados los bienes raíces o inmuebles, pero en la realidad existen otros bienes que se deben tener en cuentas como pólizas de seguros de vida, legados, bienes económicos. También la legislación vigente es muy estricta y dependiendo del país existen leyes que impiden crear testamentos con normas de cualquier manera, un ejemplo es España, donde no se puede desheredar a un hijo. Por eso este proyecto permite abrir la puerta a la investigación en este campo y deja abierta una posibilidad a futuros proyectos como los propuestos a continuación:

- Mayor aplicación de la ley vigente en España o en otros países a las normas y reglas programadas en los contratos.
- Creación de un Registro de la Propiedad más detallado y de igual forma un registro Civil que no solo recoja los datos utilizados en este Trabajo Fin de Grado, sino que refleje los registros reales.
- Implantación de procesos *Batch* en el servidor de la web con el fin de automatizar por completo la ejecución de una herencia. Un proceso *Batch* o procesamiento por lotes se trata de la ejecución de un programa de forma autónoma por una máquina sin la supervisión ni control de un usuario. Estos procesos o programas se utilizan en tareas que deben repetirse de forma periódica fuera de horas de alta densidad de

actividad por parte de usuarios, como mantenimiento nocturno, y cuyas operaciones a realizar son delicadas para llevar a cabo por un usuario debido a la posibilidad de errores al realizarlo de forma manual. La línea de trabajo que se plantea es crear procesos *Batch* para comprobar de forma periódica el estado de herencias y cuando todos los herederos hayan aceptado o renunciado a la herencia, el proceso será el encargado de ejecutar la herencia.

Otro proceso *Batch* sería la notificación a los usuarios por correo electrónico de la defunción de un testador que les ha designado como herederos.

- Trabajar en la identidad digital en Blockchain para este tipo de gestiones, al igual que existe el Documento Nacional de Identidad, de esta forma cada persona podría estar identificada mediante una cuenta en la red, aunque disponga de varias. Actualmente existen dos estándares, ERC-725 y ERC-735 [30] cuyo autor es Fabian Vogelsteller, cuyos códigos se puede consultar en la red, pero en la cabecera figura que son solo un prototipo del trabajo que se está llevando a cabo. Además, estos estándares no vinculan la cuenta a un documento identificativo legal como un DNI o número de seguridad social.
- Finalmente, trabajar en la herencia de activos económicos bancarios o en monederos de criptomonedas y otros bienes como pólizas de seguros, legados e incluso testamentos vitalicios.

Las redes descentralizadas son una tecnología que podrían cambiar grandes aspectos del día a día, facilitar los trámites como herencias, rentas u otros y así proporcionar una seguridad y transparencia en los procesos que actualmente solo se pueden hacer con personas intermediarias.

Capítulo 8. BIBLIOGRAFÍA

- [1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.” Accessed: Jul. 30, 2020. [Online]. Available: www.bitcoin.org.
- [2] “Home | ethereum.org.” <https://ethereum.org/en/> (accessed Jul. 30, 2020).
- [3] E. Davara Fernández de Marcos, *Los Smart contract*. .
- [4] “Solidity — Solidity 0.7.1 documentation.” <https://solidity.readthedocs.io/en/latest/> (accessed Jul. 30, 2020).
- [5] “Vyper — Vyper documentation.” <https://vyper.readthedocs.io/en/stable/> (accessed Jul. 30, 2020).
- [6] “HTTP | MDN.” <https://developer.mozilla.org/en-US/docs/Web/HTTP> (accessed Jul. 30, 2020).
- [7] “HTML: Hypertext Markup Language | MDN.” <https://developer.mozilla.org/en-US/docs/Web/HTML> (accessed Jul. 30, 2020).
- [8] “CSS: Cascading Style Sheets | MDN.” <https://developer.mozilla.org/en-US/docs/Web/CSS> (accessed Jul. 30, 2020).
- [9] “JavaScript | MDN.” <https://developer.mozilla.org/en-US/docs/Web/JavaScript> (accessed Jul. 30, 2020).
- [10] “PHP: Hypertext Preprocessor.” <https://www.php.net/> (accessed Aug. 18, 2020).
- [11] “MySQL.” <https://www.mysql.com/> (accessed Aug. 18, 2020).

- [12] “web3.js - Ethereum JavaScript API — web3.js 1.2.11 documentation.”
<https://web3js.readthedocs.io/en/v1.2.11/> (accessed Jul. 30, 2020).
- [13] “Ganache | Overview | Documentation | Truffle Suite.”
<https://www.trufflesuite.com/docs/ganache/overview> (accessed Jul. 30, 2020).
- [14] “Welcome to Remix documentation! — Remix, Ethereum-IDE 1 documentation.” <https://remix-ide.readthedocs.io/en/latest/> (accessed Jul. 30, 2020).
- [15] “MetaMask.” <https://metamask.io/> (accessed Aug. 18, 2020).
- [16] “Atom.” <https://atom.io/> (accessed Jul. 30, 2020).
- [17] “Navegador web Google Chrome.”
https://www.google.com/intl/es_es/chrome/ (accessed Jul. 30, 2020).
- [18] “MiniWeb.” <http://miniweb.sourceforge.net/> (accessed Jul. 30, 2020).
- [19] “WampServer, la plate-forme de développement Web sous Windows - Apache, MySQL, PHP.” <https://www.wampserver.com/en/> (accessed Aug. 18, 2020).
- [20] “Welcome! - The Apache HTTP Server Project.” <https://httpd.apache.org/> (accessed Aug. 18, 2020).
- [21] “El concepto de consenso en Blockchain, su relevancia y consecuencias,” Jul. 12, 2019. <https://santanderglobaltech.com/concepto-consenso-blockchain-relevancia-consecuencias/> (accessed Jul. 30, 2020).
- [22] “Qué es Prueba de trabajo / Proof of Work (PoW) | Bit2Me Academy.”
<https://academy.bit2me.com/que-es-proof-of-work-pow/> (accessed Jul. 30, 2020).

- [23] A. Tar, “¿Qué es Prueba de trabajo o Proof of Work (PoW)?,” Dec. 11, 2019. <https://es.cointelegraph.com/explained/proof-of-work-explained> (accessed Jul. 30, 2020).
- [24] “home - Golem.” <https://golem.network/> (accessed Aug. 06, 2020).
- [25] “Soluciones de firma electrónica para empresas | Signaturit.” <https://www.signaturit.com/es> (accessed Aug. 06, 2020).
- [26] “Asesoría Jurídica y Legal - Particulares y Empresas | DAS.” <https://www.das.es/> (accessed Aug. 06, 2020).
- [27] “Una empresa de bienes raíces de Chile registrará en Ethereum sus títulos de propiedad.” <https://www.criptonoticias.com/seguridad-bitcoin/certificacion/empresa-bienes-raices-chile-registrara-ethereum-titulos-propiedad/> (accessed Aug. 06, 2020).
- [28] España. Ministerio de Gracia y Justicia, *Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil*. 1889.
- [29] “Testamento Inteligente: privacidad y herencia digital - MLD.” <https://www.milegadodigital.com/> (accessed Aug. 06, 2020).
- [30] “ERC725 Alliance.” <https://erc725alliance.org/> (accessed Aug. 17, 2020).
- [31] C. Pérez Ramos, *Memento Práctico: Derecho de Sucesiones (Civil)*. 2019.

ANEXO I: ALINEACIÓN DEL PROYECTO CON LOS ODS

Este Trabajo Fin de Grado ha tenido en cuenta los Objetivos de Desarrollo Sostenible en los que los Estados miembros acordaron una serie de objetivos con el fin de garantizar una paz y prosperidad en la sociedad en 2030. A continuación, en la *Ilustración 40* se muestran todos los Objetivos acordados.



Ilustración 40. Objetivos de Desarrollo Sostenible

El principal objetivo que se ha perseguido en este proyecto ha sido el número nueve, dedicado a la búsqueda de la industrialización, innovación e infraestructuras. Actualmente estos enclaves/elementos desempeñan un papel fundamental para la promoción de nuevas tecnologías. Este objetivo incluye como meta el desarrollo de infraestructuras fiables y sostenibles que permitan el desarrollo económico y bienestar humano con un acceso equitativo para todos. Es por eso por lo que se ha buscado crear una aplicación, con una usabilidad apta para todas las personas que no tengan estudios de derecho para que puedan confeccionar sus testamentos sin la dependencia de terceras personas.

El desarrollo de este proyecto se basa a la tecnología de Blockchain y Smart Contract, tecnologías que requieren de una infraestructura que permitan ser utilizadas no solo para este proyecto, sino para todos los que usen estas tecnologías y al apoyarse en redes descentralizadas, no se necesita implantar una infraestructura con altos costes a base de nuevos dispositivos, sino que esta infraestructura puede implantarse a partir de los dispositivos que ya tienen los ciudadanos formando una gran red.

La tecnología de Blockchain y la investigación sobre los casos de uso y aplicaciones de los contratos inteligentes, forman parte de la innovación tecnológica y desarrollo de nuevas tecnologías de la información que proporcionan un acceso a la información de forma transparente y equitativa para todos los ciudadanos y países. Las personas pueden acceder a la información con total seguridad y con la garantía de que esta información es transparente y no ha sido corrompida por terceras personas o gobiernos.

De forma indirecta, este proyecto está involucrado con los Objetivos de Desarrollo Sostenible *1. Fin de la pobreza*, *9. Trabajo decente y crecimiento económico* y *10. Reducción de las desigualdades*. Esto es debido a que, como consecuencia de este proyecto y la implantación de una aplicación como la modelada, se eliminan multitud de gastos causados por trámites e intermediarios que existen en los modelos tradicionales de los procesos de herencia. Así mismo, en alineación con el crecimiento económico, esta aplicación es una forma de estimular la evolución de modelos fiscales y financieros tradicionales para que se pueda favorecer también a los más vulnerables.

Debido a los altos costes del proceso de herencia, se crea una desigualdad en la que muchas veces los herederos no pueden disfrutar de aquellos bienes que le son legados al no disponer de recursos económicos para hacer frente a las costas de los trámites de una herencia. Mediante la reducción de costes durante el proceso, se crea una situación igualitaria para todos los ciudadanos pudiendo estos hacer frente a los procesos de herencia con mayor facilidad.

Aun así, tal y como se indica al final de la memoria de este Trabajo Fin de Grado en el Capítulo 7. , se abre una nueva línea para futuros trabajos en favor del desarrollo de estas

tecnologías que su vez permiten continuar trabajando en alineación con los Objetivos de Desarrollo Sostenible permitiendo la innovación, acercamiento de la información a los ciudadanos y proporcionando una mayor igualdad económica.

ANEXO II: MANUAL DE INSTALACIÓN

Este anexo recoge un manual de instalación para la puesta en marcha de la aplicación desarrollada en este Trabajo Fin de Grado.

A II.1 CONFIGURACIÓN DE GANACHE

1. Se comienza abriendo la aplicación Ganache instalada previamente en el equipo y creando una nueva red, o abriendo una ya existente:
 - a. Crear una nueva red configurando el nombre, cuentas y puerto de acceso:

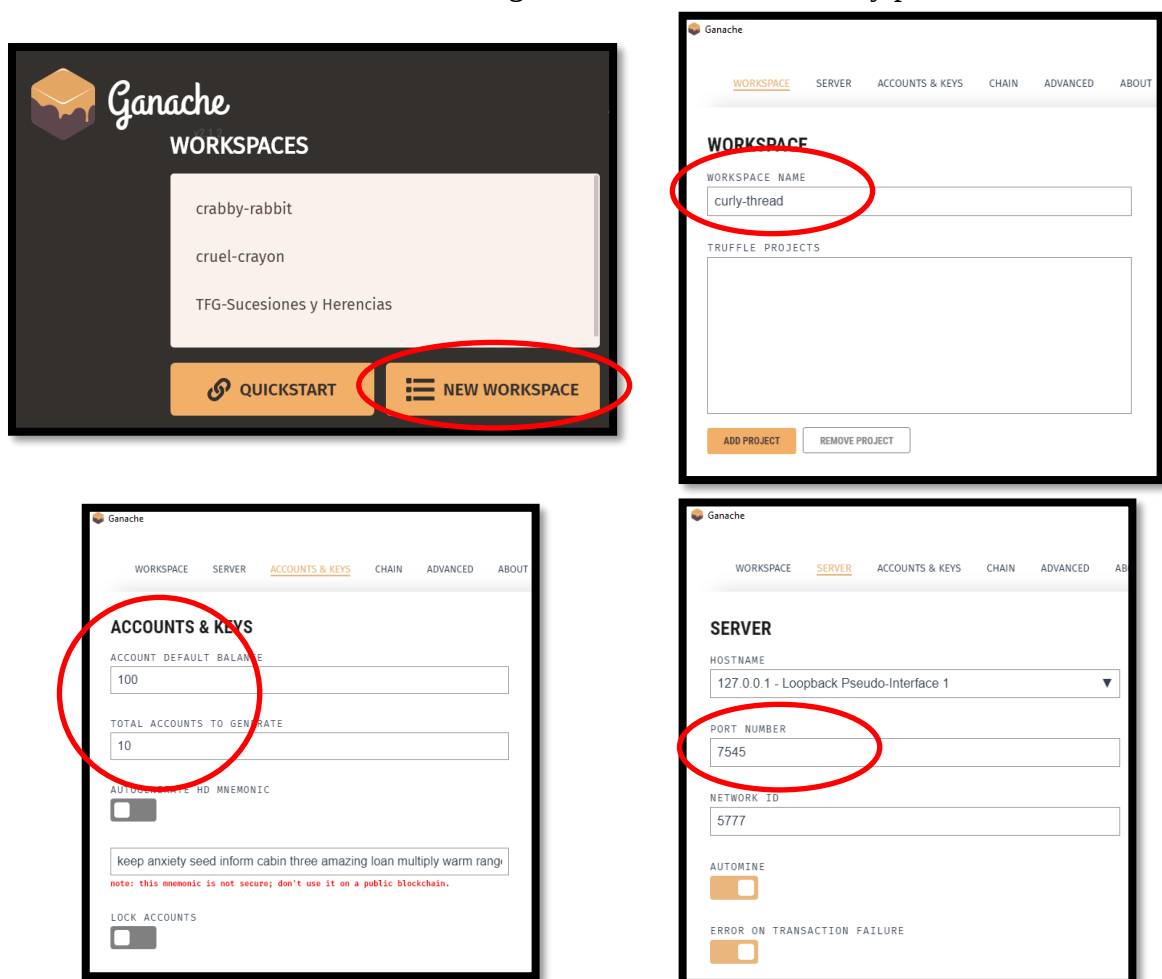


Ilustración 41. Configuración de Ganache (a)

b. Abrir una red ya existente:

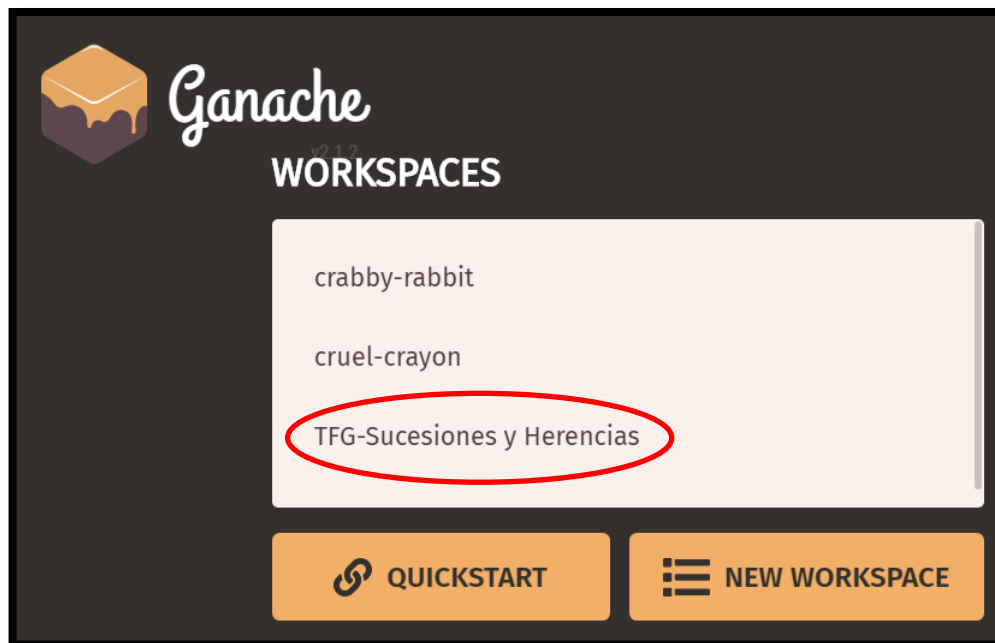


Ilustración 42. Selección de una red existente en Ganache (b)

2. A continuación, se nos abrirá la red donde podremos ver información de la red y las cuentas/nodos simulados.

ACCOUNTS	BLOCKS	TRANSACTIONS	CONTRACTS	EVENTS	LOGS	UPDATE AVAILABLE	SEARCH FOR BLOCK
CURRENT BLOCK 519	GAS PRICE 2000000000	GAS LIMIT 6721975	HARDFORK PETERSBURG	NETWORK ID 5777	RPC SERVER HTTP://127.0.0.1:7545	MINING STATUS AUTOMINING	WORKSPACE TFG-SUCESIONES Y HERENCIAS
ADDRESS 0xA6a2DC761EEDcE3Ed8dD274F10C2CB67eF18b5C4	BALANCE 95.40 ETH	TX COUNT 275	INDEX 0				
ADDRESS 0x09Af12DAD9B326B88C84C58b314CA4Fcce838463	BALANCE 99.88 ETH	TX COUNT 25	INDEX 1				
ADDRESS 0x8277cAef1735cB9486A0C38F79F7938cE4230f3f	BALANCE 99.98 ETH	TX COUNT 4	INDEX 2				
ADDRESS 0x440f67C8Ca4670F956F78FaF373052917C709583	BALANCE 99.98 ETH	TX COUNT 11	INDEX 3				
ADDRESS 0x07802C6E53D5B91CFD6C76Ab205f6Aa93f34eb96	BALANCE 99.96 ETH	TX COUNT 16	INDEX 4				

Ilustración 43. Aplicación Ganache en ejecución simulando una red

A II.2 CONFIGURACIÓN DE LOS SERVICIOS WAMPSEVER

1. Una vez instalado los servicios de WampServer, ejecutamos la aplicación:

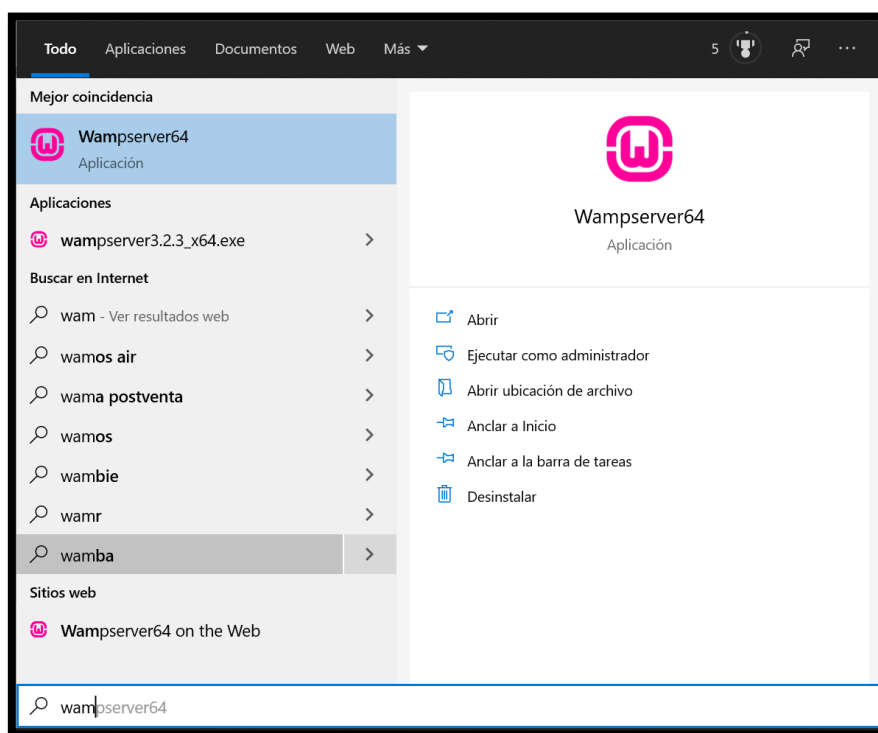


Ilustración 44. Inicio de la aplicación WampServer

2. Con la aplicación iniciada, pulsamos sobre el icono de WampServer donde se desplegarán todos los componentes de la aplicación.

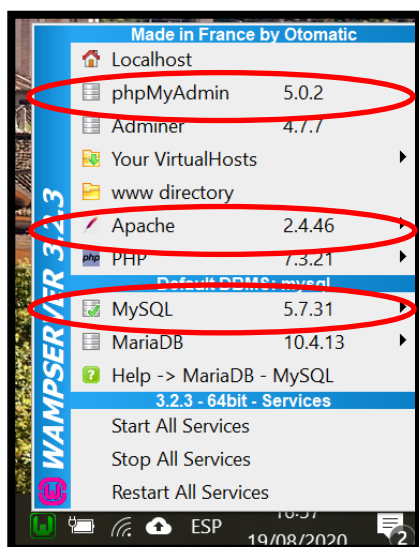


Ilustración 45. Servicios de WampServer

Aquí podemos ver todos los servicios que contiene esta aplicación, en este proyecto solo se usarán:

- phpMyAdmin
- Apache
- MySQL

Procedamos a la configuración necesaria de cada uno.

A II. 2.1 CONFIGURACIÓN DE PHPMyADMIN Y MYSQL

A continuación, se detallan los pasos para poner en marcha la base de datos de MySQL a partir del administrador phpMyAdmin:

1. Pulsamos sobre phpMyAdmin, en *Ilustración 45. Servicios de WampServer*.
2. Se nos despliega el entorno en el navegador web y pulsamos sobre “importar”:

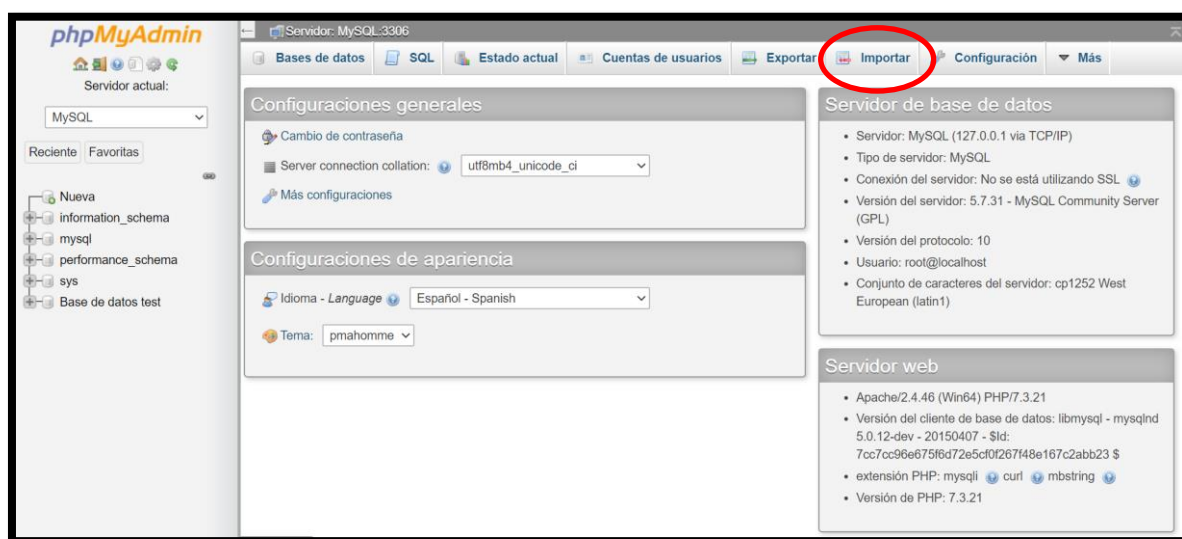


Ilustración 46. Entorno de phpMyAdmin

3. Seleccionamos el archivo “tfg_manuelmda.sql” y pulsamos “continuar”.

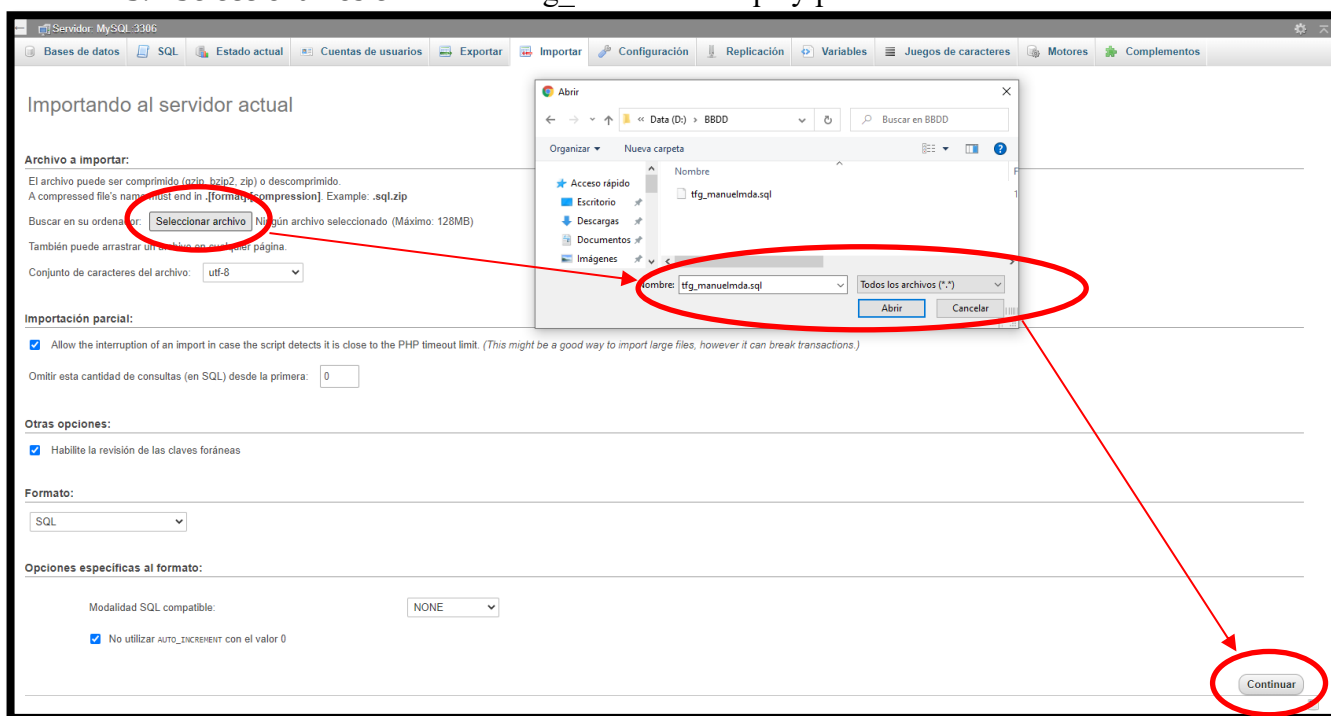


Ilustración 47. Importación de base de datos

4. Para finalizar, se podrá ver en la parte izquierda del administrador de bases de datos la BBDD importada y se podrá acceder a ella.

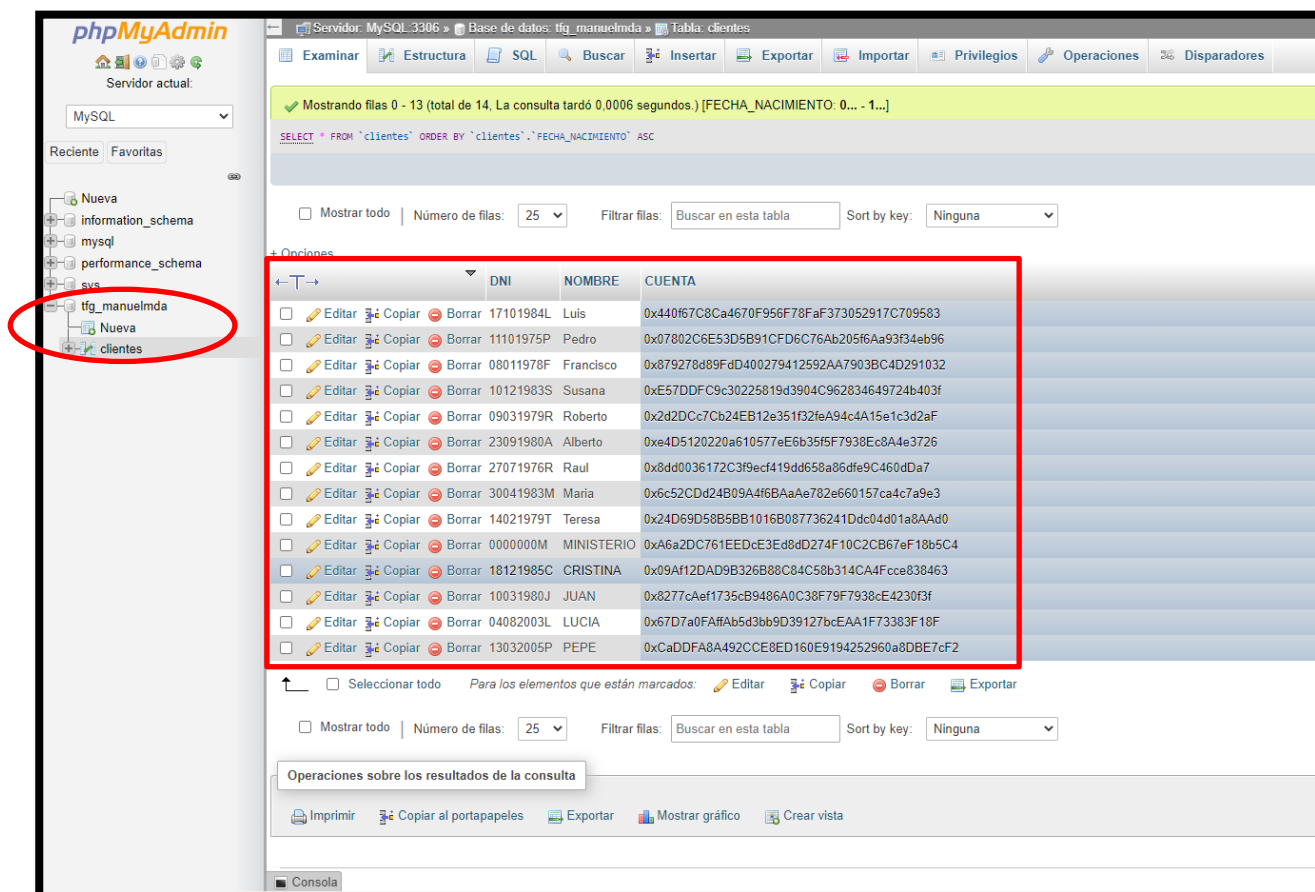


Ilustración 48. BBSS importada

A II. 2.2 CONFIGURACIÓN DEL SERVIDOR APACHE Y HOSTS VIRTUALES

1. En primer lugar, para poder acceder a las páginas de los usuarios Clientes y el usuario Ministerio a través de los dominios “tfg.mitestamento.com” y “tfg.ministerio.com” accedemos al archivo “hosts” ubicado en la ruta “C:\Windows\System32\drivers\etc”
2. Añadimos las relaciones marcadas en rojo en *Ilustración 49. Contenido del archivo "hosts"* para redirigir dichos dominios.

Nota: Al ser un proyecto que no se puede desplegar para uso real, se está almacenando la web en local.

```
1 # Copyright (c) 1993-2009 Microsoft Corp.
2 #
3 # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
4 #
5 # This file contains the mappings of IP addresses to host names. Each
6 # entry should be kept on an individual line. The IP address should
7 # be placed in the first column followed by the corresponding host name.
8 # The IP address and the host name should be separated by at least one
9 # space.
10 #
11 # Additionally, comments (such as these) may be inserted on individual
12 # lines or following the machine name denoted by a '#' symbol.
13 #
14 # For example:
15 #
16 # 102.54.94.97 rhino.acme.com # source server
17 # 38.25.63.10 x.acme.com # x client host
18
19 # localhost name resolution is handled within DNS itself.
20 # 127.0.0.1 localhost
21 # ::1 localhost
22
23 127.0.0.1 tfg.mitestamento.com
24 127.0.0.1 tfg.ministerio.com
```

Ilustración 49. Contenido del archivo "hosts"

3. Abrimos el archivo "httpd-vhosts.conf" en la ruta de instalación de WampServer "D:\wamp64\bin\apache\apache2.4.46\conf\extra".
4. Añadimos las siguientes líneas marcadas en rojo en la Ilustración 50.

```
1 # Virtual Hosts
2 #
3 <VirtualHost *:80>
4     ServerName localhost
5     ServerAlias localhost
6     DocumentRoot "${INSTALL_DIR}/www"
7     <Directory "${INSTALL_DIR}/www/">
8         Options +Indexes +Includes +FollowSymLinks +MultiViews
9         AllowOverride All
10        Require local
11    </Directory>
12 </VirtualHost>
13
14 <VirtualHost *:80>
15     DocumentRoot "D:/wamp64/www/TFG/ministerio"
16     ServerName tfg.ministerio.com
17     ServerAlias tfg.ministerio.com
18     <Directory "D:/wamp64/www/TFG/ministerio">
19
20 </VirtualHost>
21
22 <VirtualHost *:80>
23     DocumentRoot "D:/wamp64/www/TFG/cliente"
24     ServerName tfg.mitestamento.com
25     ServerAlias tfg.mitestamento.com
26     <Directory "D:/wamp64/www/TFG/cliente">
27
28 </VirtualHost>
29
```

Ilustración 50. Contenido del archivo "httpd-vhosts.conf"

5. Finalmente, añadimos a la carpeta “www” localizada en la ruta de instalación de WampServer “D:\wamp64\www” la carpeta “TFG” que contiene el *front-end* de la aplicación web desarrollada en este Trabajo Fin de Grado.

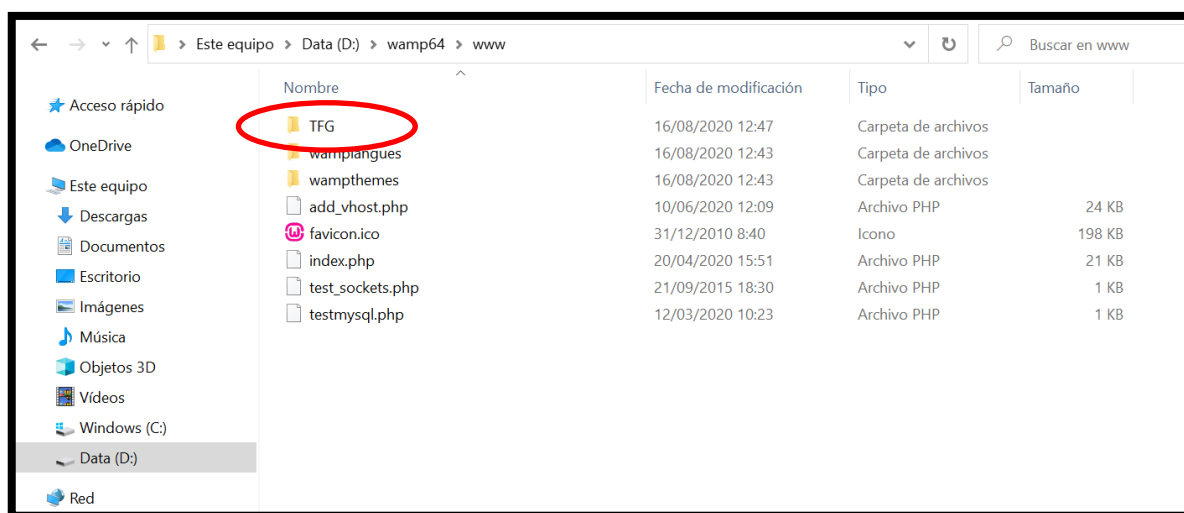


Ilustración 51. Contenido de la carpeta "www"

6. Reiniciamos todos los servicios y al abrir el navegador web con el dominio “tfg.mitestamento.com” ó “tfg.ministerio.com” se accederá al *front-end* de la aplicación desarrollada.

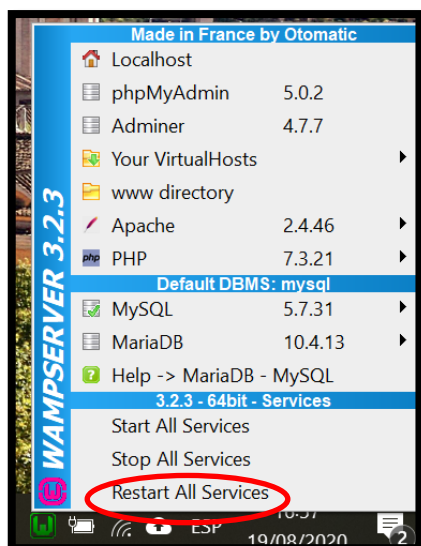


Ilustración 52. Reinicio de servicios

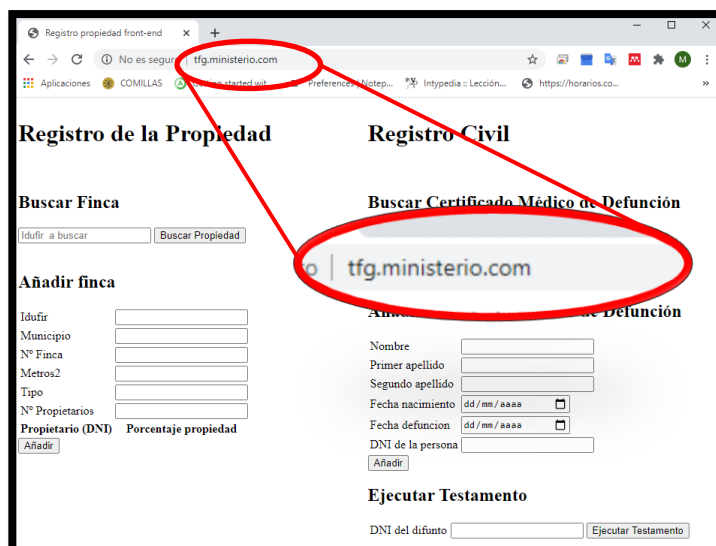


Ilustración 53. Dominio de la aplicación

A II.3 DESPLIEGUE DE LOS CONTRATOS DESDE REMIX EN GANACHE

Con la red de ganache configurada en A II. 1 *Configuración de ganache*

1. Abrimos Remix IDE en un navegador web y en su explorador de archivos cargamos “RegistroCivil.sol”, “Herencia.sol”, “RegistroPropiedad.sol”.

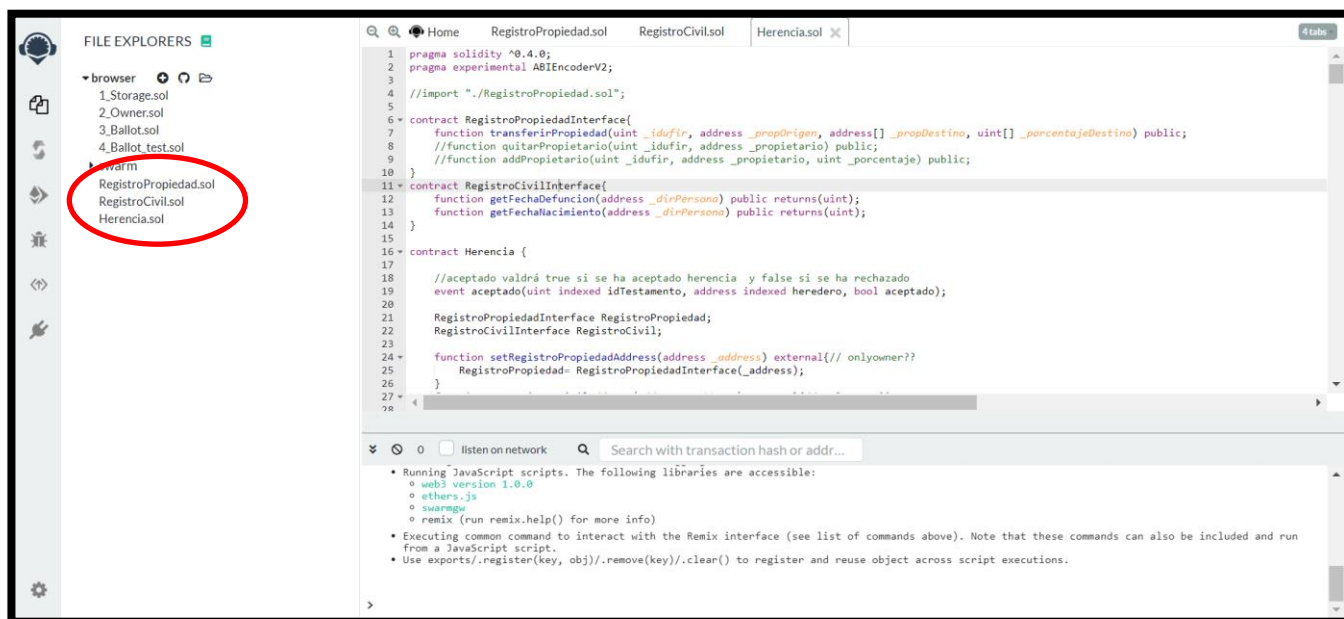


Ilustración 54. Remix IDE

2. En el IDE abrimos en la izquierda el menú “Deploy & run transactions”.

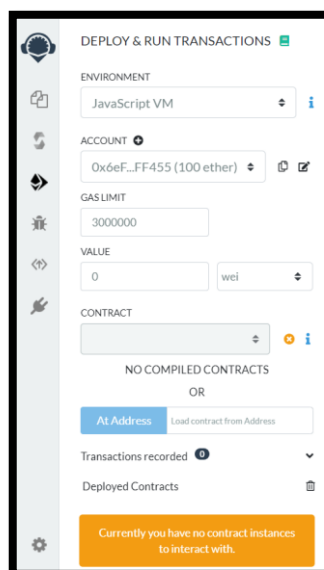


Ilustración 55. Menú “Deploy & run transactions”

- En el menú desplegado, cambiamos “Enviroment” a “Web 3 provider” e introducimos el puerto donde configuramos la red de blockchain de ganache en el apartado *A II. 1 Configuración de ganache*.

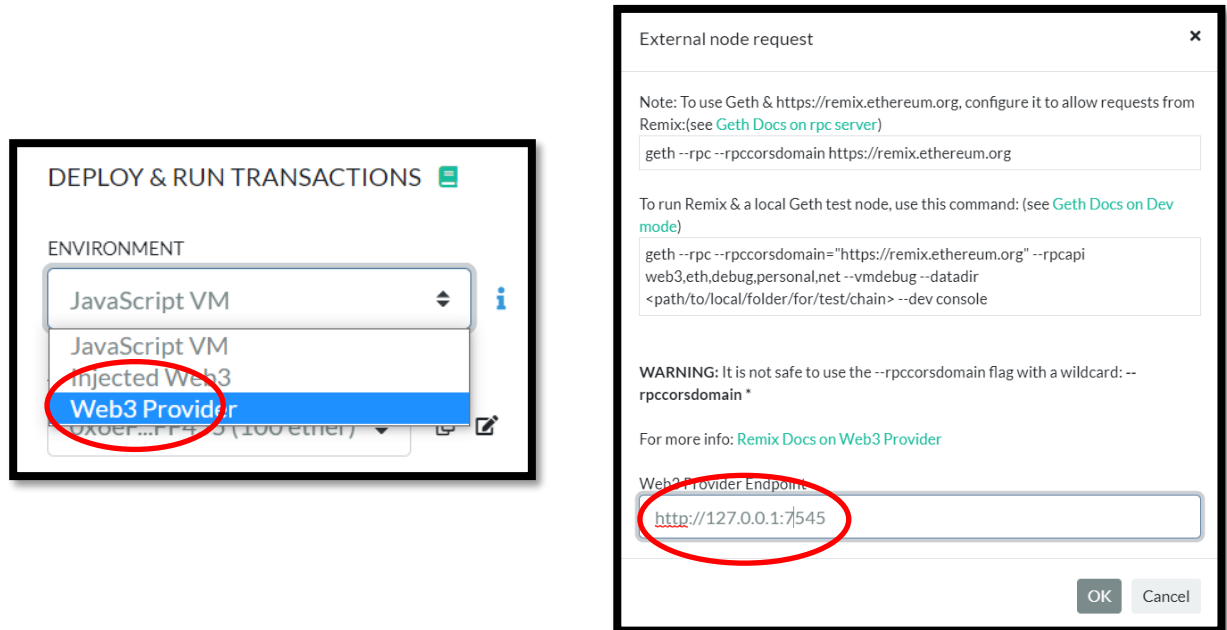


Ilustración 56. Configuración de conexión con red de Ganache

- Al aceptar, el IDE se conectará a la red simulada con Ganache y se podrán ver las cuentas de dicha red:

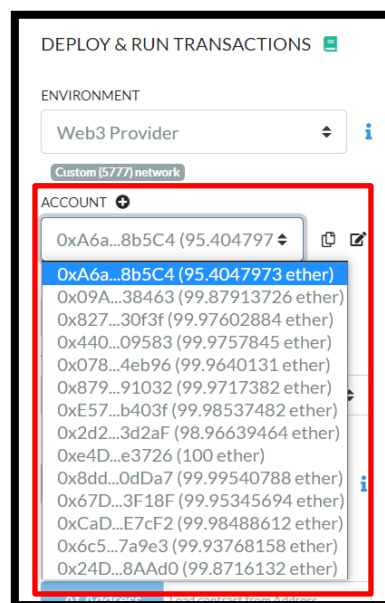


Ilustración 57. Cuentas de Ganache visualizadas en Remix IDE

- En cada uno de los tres contratos compilamos pulsando la combinación de teclas “ctrl+s” y en el menú “Deploy & run transactions” pulsamos en “deploy” para desplegar el contrato sobre la red.

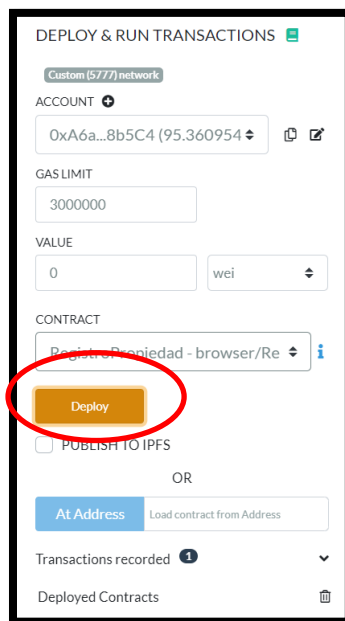


Ilustración 58. Despliegue de contratos

- Una vez desplegados los tres contratos, se visualizarán junto con su dirección en la parte baja del menú (Azul). En la consola del IDE podremos ver cada una de las tres transacciones realizadas (Verde).

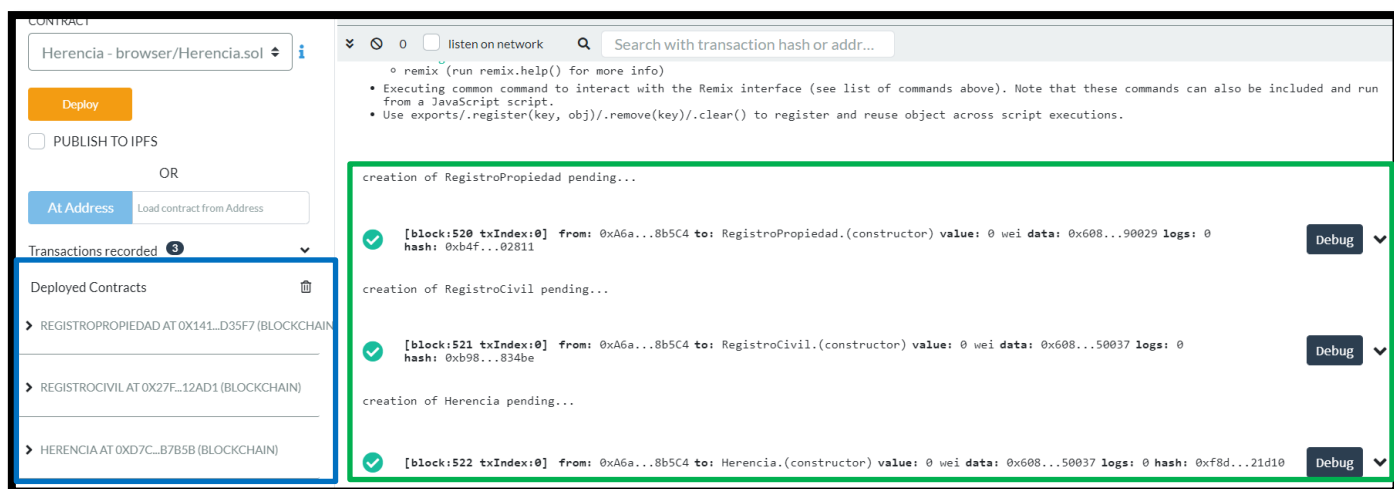


Ilustración 59. Transacciones realizadas durante el despliegue

7. En cada instancia de los contratos creados, podemos desplegar su pestaña mostrando todos los métodos de estos (Azul). También podemos copiar (Verde) la dirección de cada uno. Copiamos y reservamos cada una de las tres direcciones pues las necesitaremos más adelante.

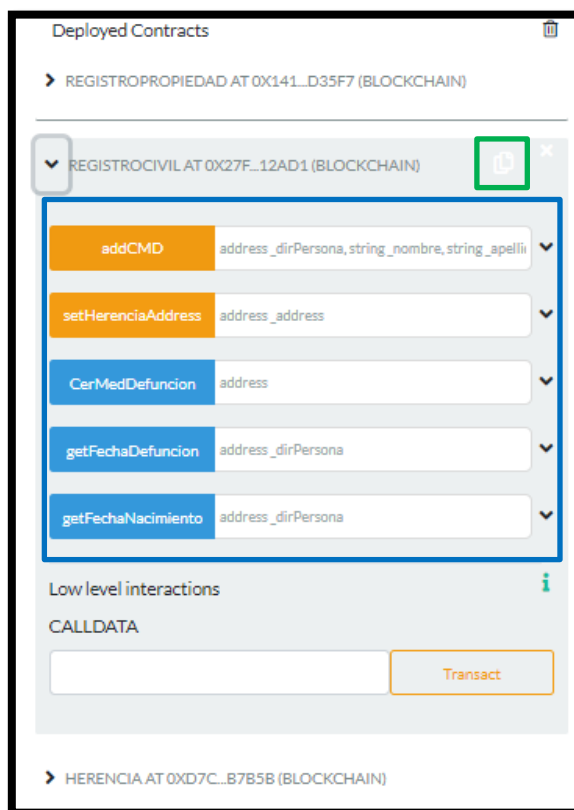


Ilustración 60. Detalle de un contrato desplegado en Remix IDE

8. Una vez que hemos copiado y reservado las tres direcciones, necesitamos poner en comunicación a los contratos entre ellos. En concreto, Herencia.sol debe tener comunicación con RegistroPropiedad.sol y RegistroCivil.sol y, por otro lado, RegistroCivil.sol debe poder contactar con Herencia.sol. Para ellos se han creado unos métodos llamados “setNombreContratoAddress(address _address)” en cada contrato. Lo que hacemos es pegar cada dirección reservada en la función pertinente tal y como se muestra en la Ilustración 61 y pulsamos sobre el botón naranja del propio método para ejecutar la función.

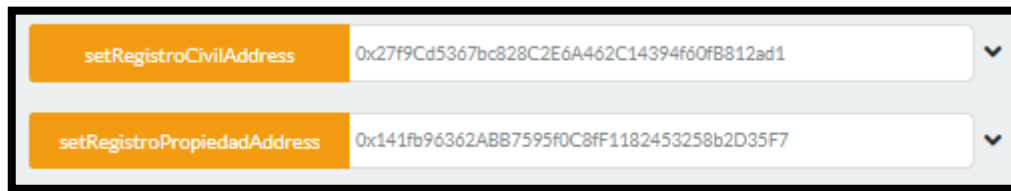


Ilustración 61. Métodos para configurar direcciones de las interfaces

9. Reservamos las direcciones para el siguiente apartado.

A II. 4 CONFIGURACIÓN DE COMUNICACIÓN ENTRE BACK-END Y FRONT-END

Una vez desplegados los contratos en la red de ganache, el *front-end* debe poder comunicarse con los contratos, *back-end*, para ello, teniendo la copia de las direcciones de los contratos desplegados:

1. Abrimos los archivos “main.js” de las rutas “D:\wamp64\www\TFG\cliente\js” y “D:\wamp64\www\TFG\ministerio\js”. Debajo de la primera función “startApp()”, encontramos definidas tres variables que hacen referencia a los tres contratos. Rellenamos cada variable con el contrato correspondiente tal y como se muestra a continuación:

```
/* Funcion para comenzar con el funcionamiento de la app*/  
function startApp() {  
    // Variables que contiene la direccion del SmartContract  
    var addressHerencia = "0xd7C9457f19b836c0fb5CCcaE81afabD391B7b5b";  
    var addressRegistroPropiedad = "0x141fb96362ABB7595f0C8fF1182453258b2D35F7";  
    var addressRegistroCivil = "0x27f9Cd5367bc828C2E6A462C14394f60fB812ad1";
```

Ilustración 62. Configuración de variables que definen direcciones de contratos

A II. 5 INSTALACIÓN Y CONFIGURACIÓN DE METAMASK

1. Instalamos MetaMask en nuestro navegador.
2. Una vez instalado, se nos abre la pantalla de inicio

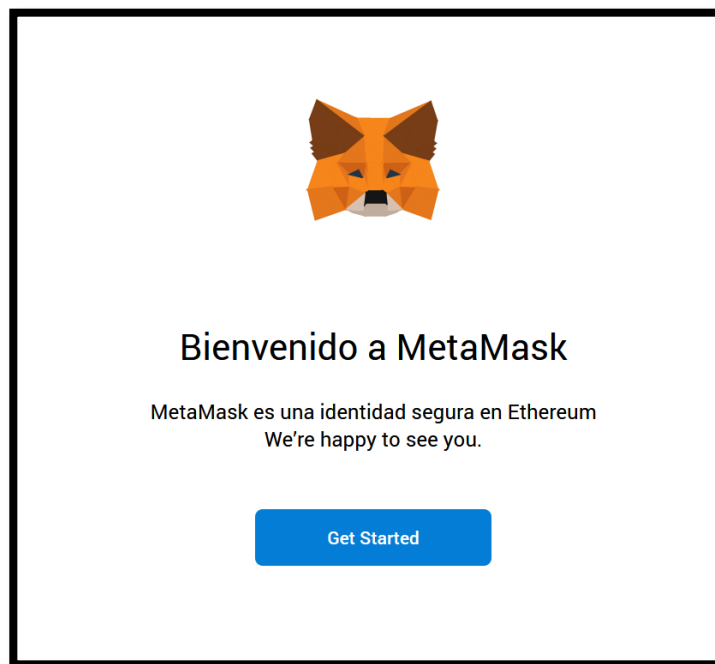


Ilustración 63. Pantalla de inicio en MetaMask

3. Pulsamos "Get Started" y en el caso de no tener una cartera para probar el funcionamiento, creamos una:

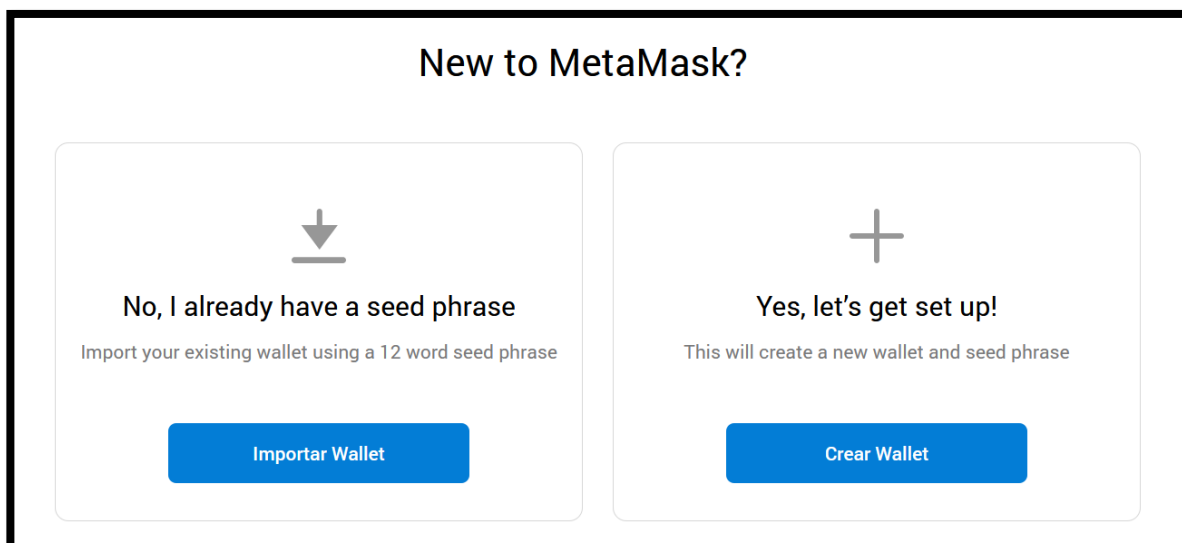


Ilustración 64. Selección inicial en MetaMask

4. Introducimos una contraseña para nuestra cartera:

Términos de uso'. At the bottom is a blue button labeled 'Crear'." data-bbox="356 190 666 396"/>

Ilustración 65. Creación de contraseña para la cartera

5. Se nos muestra la frase secreta de *backup*, esta frase nunca debe perderse ni olvidarse. Para verla, pinchar sobre el candado:

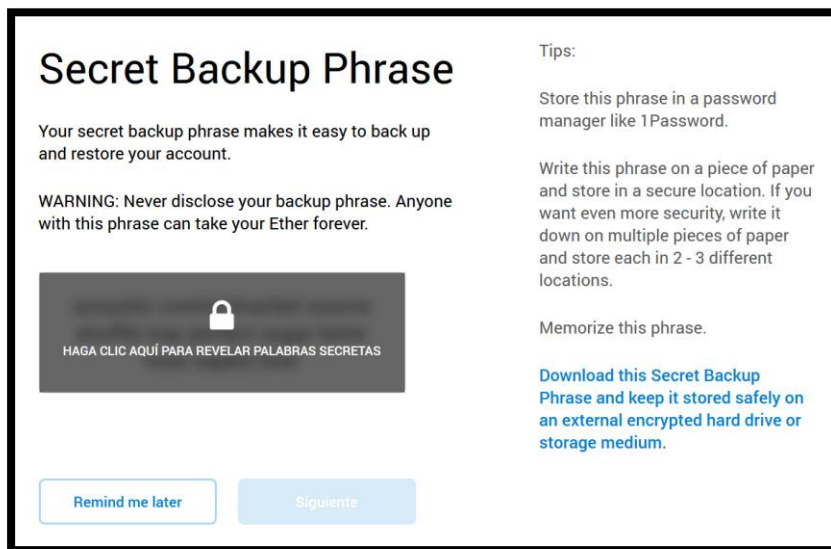


Ilustración 66. Frase secreta de backup

6. Para comprobar el paso anterior, es necesario introducir las palabras en el orden correcto.

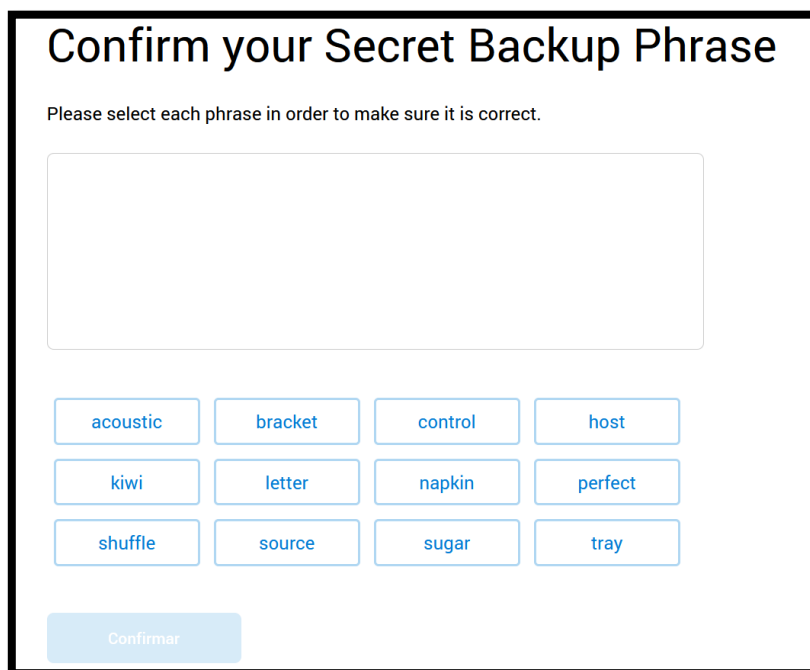


Ilustración 67. Confirmación de frase secreta

7. Ya se ha creado la billetera. A continuación, abrimos MetaMask en la esquina superior derecha de nuestro navegador (Rojo) y veremos la primera cuenta creada por defecto (Azul). Para conectarnos a la red de blockchain simulada con Ganache pulsamos sobre el icono mostrado en la imagen (Verde).

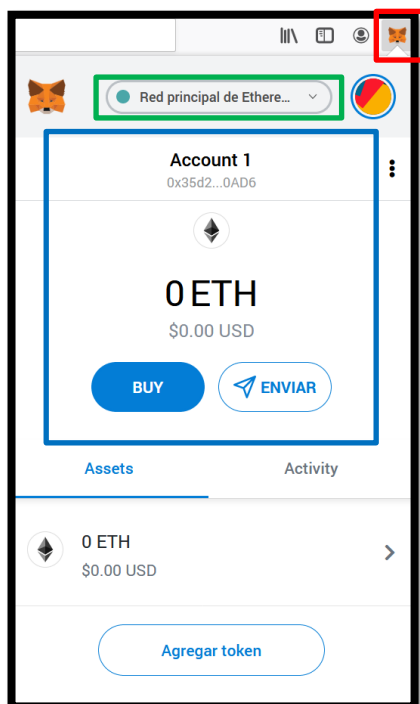


Ilustración 68. Pantalla inicial de MetaMask

8. Seleccionamos “RPC personalizada” y configuramos la red como se muestra en la imagen, introduciendo la dirección IP y el puerto con el que se configuró la red en el apartado A II. 1 *Configuración de ganache*.

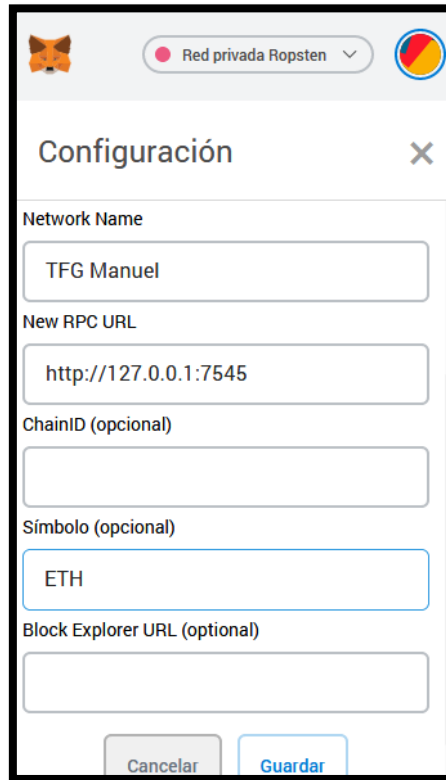


Ilustración 69. Configuración de red Ganache en MetaMask

9. Elegimos las cuentas que deseemos usar, en este ejemplo se ha elegido la cuenta que corresponde a CRISTINA que es la cuenta mostrada a continuación

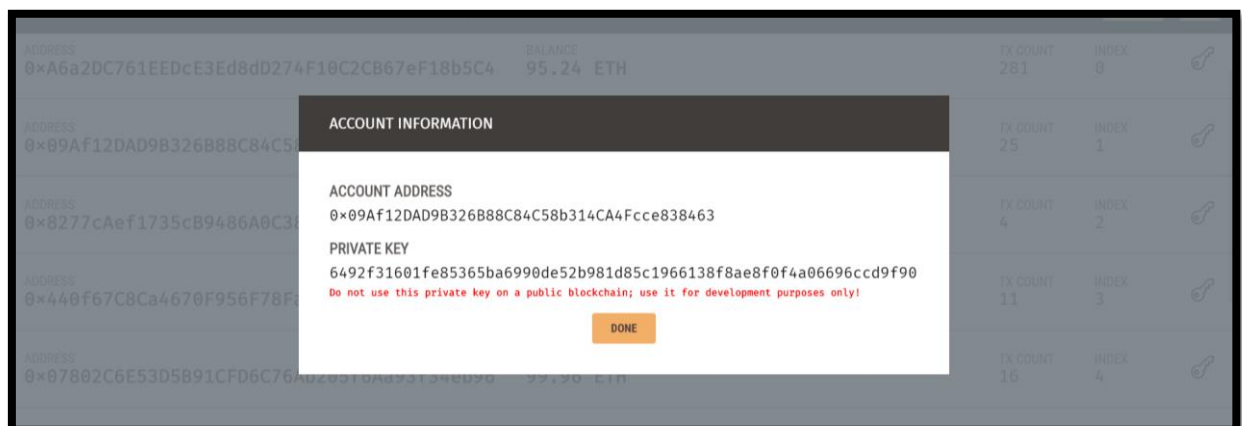


Ilustración 70. Detalle de información de la cuenta index 2 de Ganache

10. Por último, importamos la cuenta siguiendo los pasos mostrados en *Ilustración 71* e ingresando cuando se solicite la clave privada de a cuenta a importar:

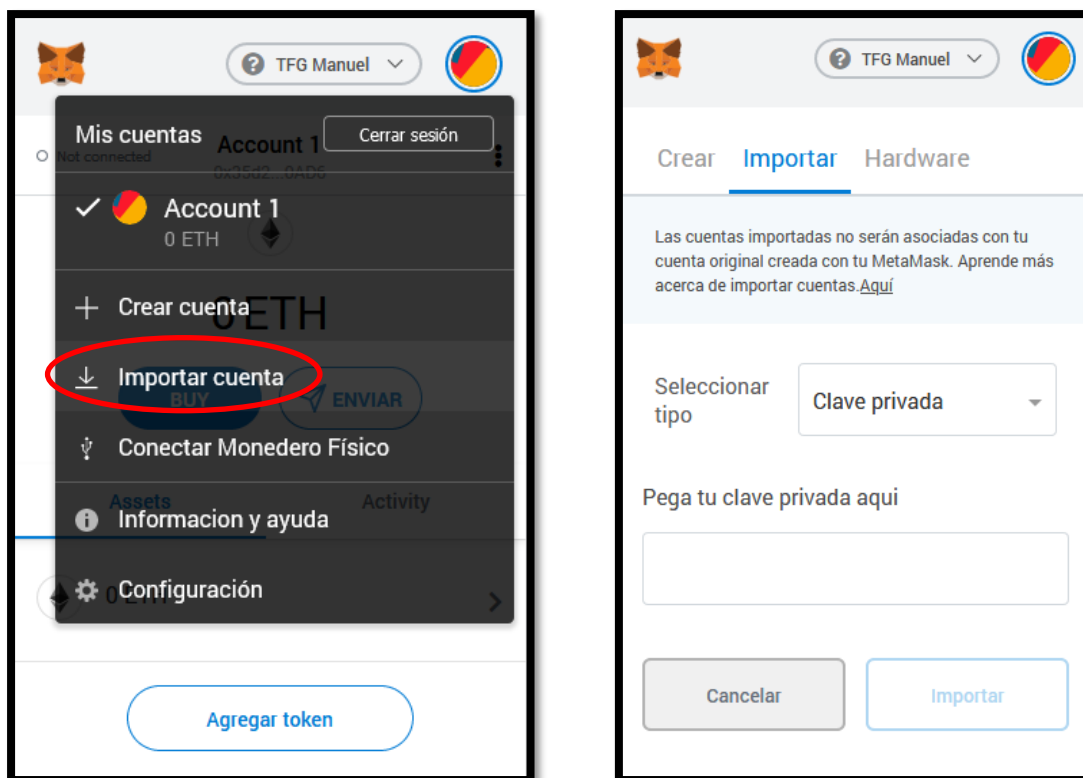


Ilustración 71. Importación de una cuenta en MetaMask

11. Si introducimos la URL “tfg.ministerio.com” podemos observar que funciona correctamente ya que arriba a la izquierda se muestra la información de la cuenta del usuario conectado:

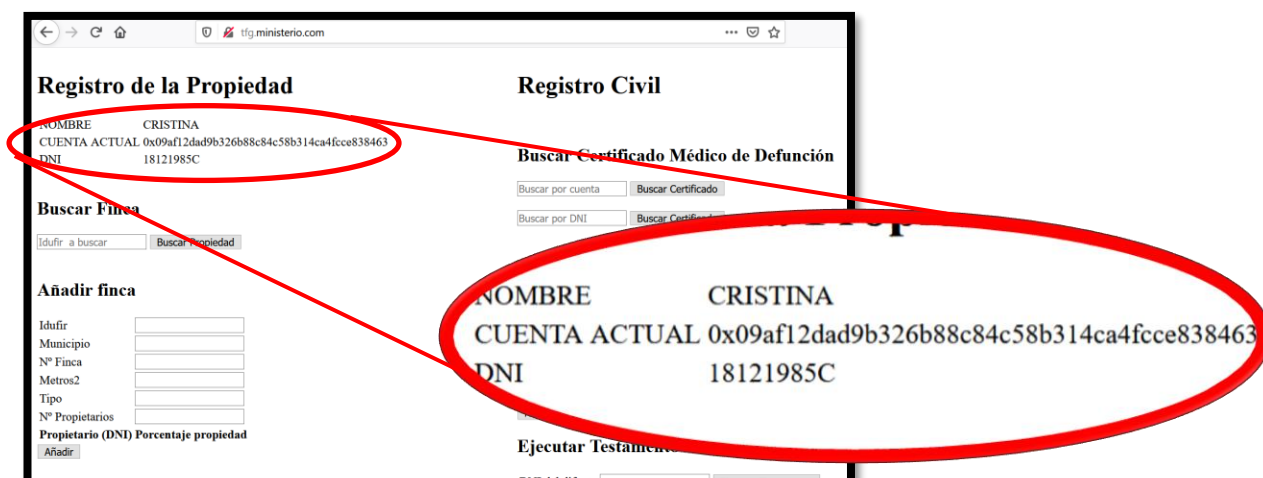


Ilustración 72. Captura de la aplicación en funcionamiento

ANEXO III: MANUAL DEL USUARIO

Este anexo recoge un manual de usuario para que los usuarios puedan interactuar y usar la aplicación desarrollada en este Trabajo Fin de Grado.

La aplicación consta de dos partes separadas en dos URLs o dominios diferentes:

- **tfg.ministerio.com:** Desde esta parte de la aplicación, el usuario “Ministerio” podrá administrar el Registro de la Propiedad y el Registro Civil.
- **tfg.mitestamento.com:** Desde esta parte de la aplicación, cualquier usuario podrá escribir o crear testamentos y consultar los ya creados. También podrán consultar trámites pendientes de herencias que deben aceptar o renunciar.

A III.1 INICIO DE LA APLICACIÓN

Para iniciar la aplicación:

1. Abrir un navegador web instalado en nuestro dispositivo.
2. Asegurarse de que tenemos una billetera de criptomonedas (MetaMask) instalada en nuestro navegador. Si no es así consúltase *A II. 5 Instalación y configuración de MetaMask*.
3. Una vez que tenemos el navegador abierto y MetaMask listo, ingresamos la URL “tfg.mitestamento.com” ó “tfg.ministerio.com” y se nos redireccionará a la aplicación web tal y como se muestra en *Ilustración 73* e *Ilustración 74*.

Ilustración 73. Vista de "tfg.ministerio.com"

Ilustración 74. Vista de "tfg.ministerio.com"

A II. 2 TFG.MINISTERIO.COM

En esta sección se detalla el funcionamiento de “tfg.ministerio.com”. Esta parte de la aplicación está dividida en dos secciones, por un lado, el Registro de la Propiedad y por el otro el Registro Civil.

A III. 2.1 REGISTRO DE LA PROPIEDAD

En el Registro de la Propiedad se podrán realizar dos acciones diferentes, por un lado, la consulta de un inmueble en el Registro de la Propiedad a partir del Idufir identificativo de dicho inmueble, y por otro lado el registro de una propiedad rellenando los datos requeridos.

A III. 2.1.1 Consulta de una propiedad o inmueble

Para realizar una consulta al Registro de la Propiedad y obtener la información de un inmueble:

1. Introducimos el Idufir que deseamos consultar y pulsamos “Buscar Propiedad”:

Buscar Finca

Idufir: 9890
 Municipio: Candamo
 Nª Finca: 23
 M2: 256
 Tipo: Chalet

Propietarios	DNI	Cuentas	Porcentajes
Maria	30041983M	0x6c52CDd24B09A4f6BAaAe782e660157ca4c7a9e3	60
Teresa	14021979T	0x24D69D58B5BB1016B087736241Ddc04d01a8AAAd0	40

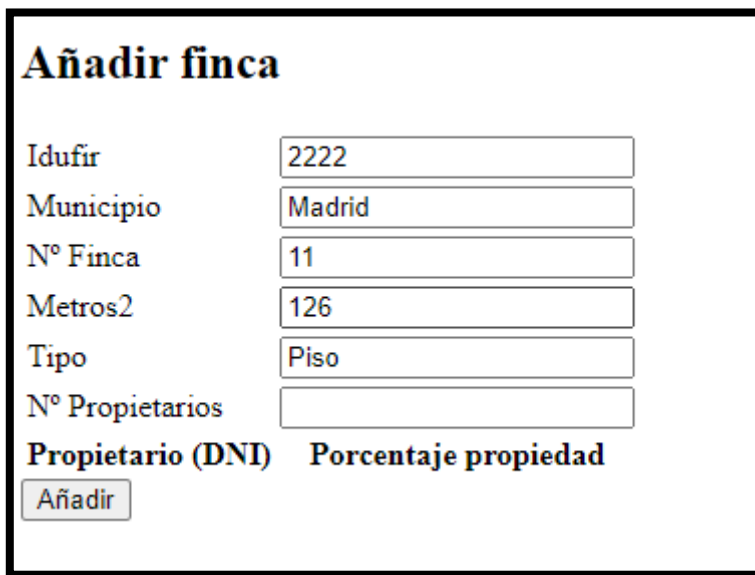
Ilustración 75. Consulta realizada de una finca (Idufir: 9890)

Como podemos ver se muestra la información de la finca y una tabla con los datos principales de los propietarios.

A III. 2.1.2 Registro de una propiedad o inmueble

Para realizar el registro de una propiedad en el Registro de la Propiedad:

1. Introducimos los datos de la finca:

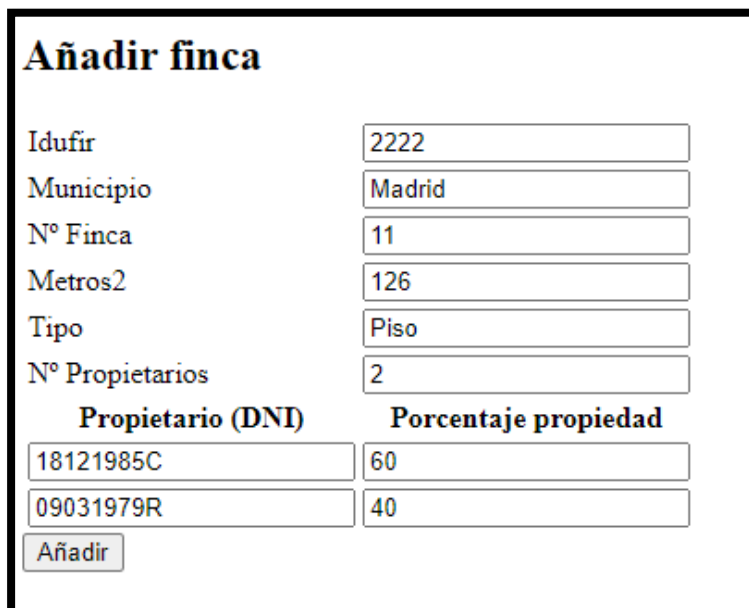


Añadir finca

Idufir	2222
Municipio	Madrid
N° Finca	11
Metros2	126
Tipo	Piso
N° Propietarios	
Propietario (DNI)	Porcentaje propiedad
Añadir	

Ilustración 76. Introducción de datos de una finca

2. Introducimos el número de propietarios y automáticamente se despliega una tabla para rellenar con la información de cada propietario (DNI y porcentaje de la finca)



Añadir finca

Idufir	2222
Municipio	Madrid
N° Finca	11
Metros2	126
Tipo	Piso
N° Propietarios	2
Propietario (DNI)	Porcentaje propiedad
18121985C	60
09031979R	40
Añadir	

Ilustración 77. Introducción de datos de los propietarios de una finca

3. Pulsamos aceptar y se nos abre MetaMask para confirmar la transacción:

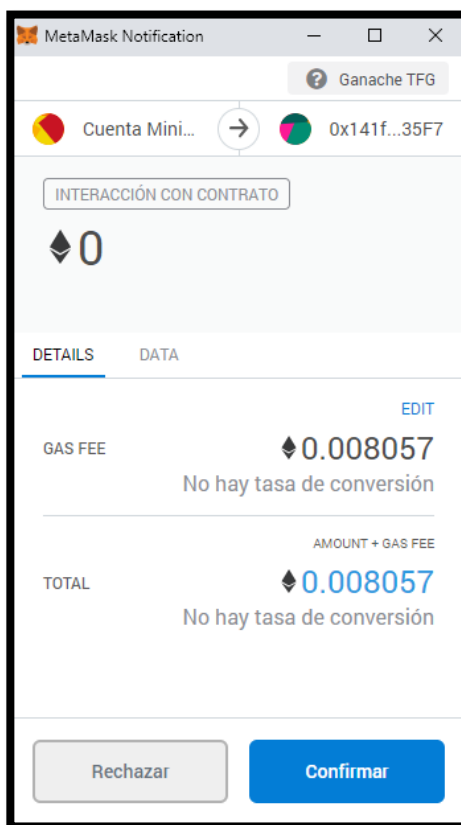


Ilustración 78. Confirmación de transacción del registro de una finca

4. Al confirmar la transacción la finca se habrá añadido la finca al registro

A III. 2.2 REGISTRO CIVIL

En el Registro Civil se podrán realizar tres acciones diferentes, la búsqueda de un Certificado Médico de Defunción, el registro de un Certificado Médico de defunción rellenando los datos requeridos y por último la ejecución de un testamento.

A III. 2.2.1 Consulta de un Certificado Médico de Defunción

La consulta de un Certificado Médico de Defunción (CMD) puede realizarse a partir de la cuenta Ethereum del difunto o de su DNI:



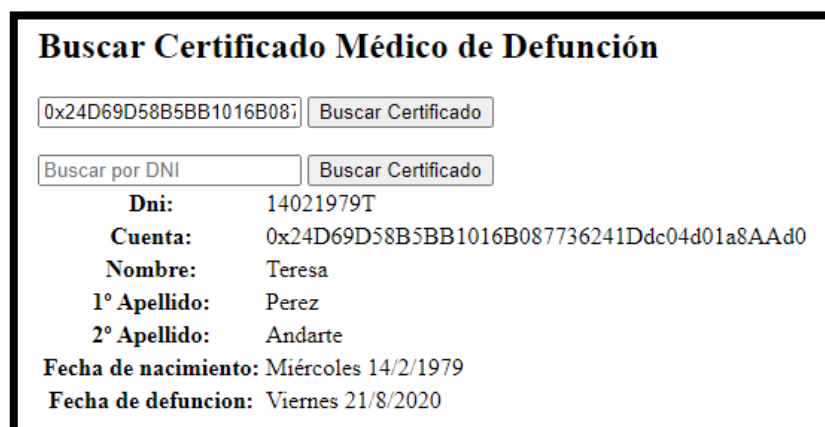
Buscar Certificado Médico de Defunción

Buscar por cuenta Buscar Certificado

Buscar por DNI Buscar Certificado

Ilustración 79. Cuadro de búsqueda de un CMD

- a) Introducimos la cuenta del difunto y pulsamos sobre “Buscar Certificado”



Buscar Certificado Médico de Defunción

0x24D69D58B5BB1016B087 Buscar Certificado

Buscar por DNI Buscar Certificado

Dni: 14021979T
Cuenta: 0x24D69D58B5BB1016B087736241Ddc04d01a8AAAd0
Nombre: Teresa
1º Apellido: Perez
2º Apellido: Andarte
Fecha de nacimiento: Miércoles 14/2/1979
Fecha de defuncion: Viernes 21/8/2020

Ilustración 80. Búsqueda de CMD por cuenta

- b) Introducimos el DNI del difunto y pulsamos sobre “Buscar Certificado”



Buscar Certificado Médico de Defunción

Buscar por cuenta Buscar Certificado

14021979T Buscar Certificado

Dni: 14021979T
Cuenta: 0x24D69D58B5BB1016B087736241Ddc04d01a8AAAd0
Nombre: Teresa
1º Apellido: Perez
2º Apellido: Andarte
Fecha de nacimiento: Miércoles 14/2/1979
Fecha de defuncion: Viernes 21/8/2020

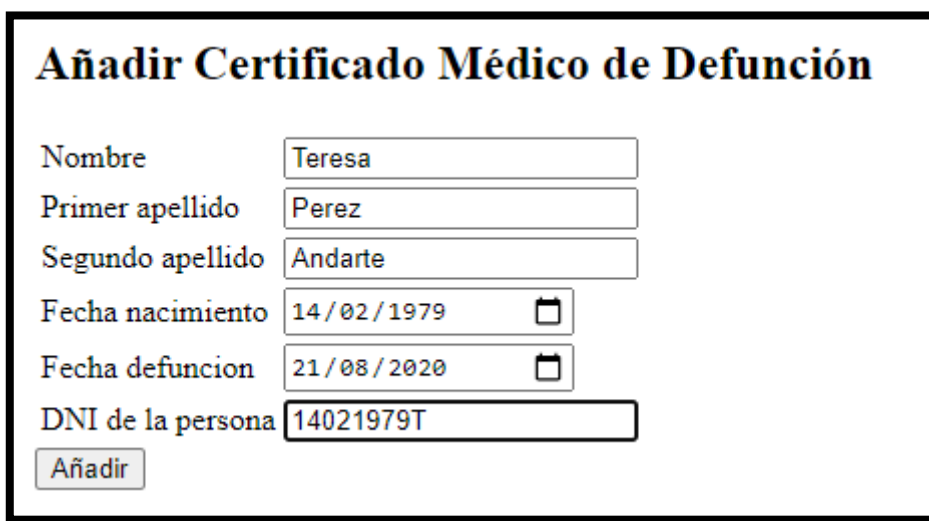
Ilustración 81. Búsqueda de CMD por cuenta

El resultado de ambas búsquedas es el mismo ya que es la misma persona

A III. 2.2.2 Registro de un Certificado Médico de Defunción

Para registrar una defunción y, por lo tanto, añadir un Certificado Médico de Defunción (CMD) al Registro Civil:

1. Rellenamos los datos pertinentes del difunto:



Añadir Certificado Médico de Defunción

Nombre	Teresa
Primer apellido	Perez
Segundo apellido	Andarte
Fecha nacimiento	14/02/1979
Fecha defuncion	21/08/2020
DNI de la persona	14021979T
Añadir	

Ilustración 82. Registro de un nuevo CMD

2. Pulsamos “Añadir” y se nos abre MetaMask para confirmar la transacción:

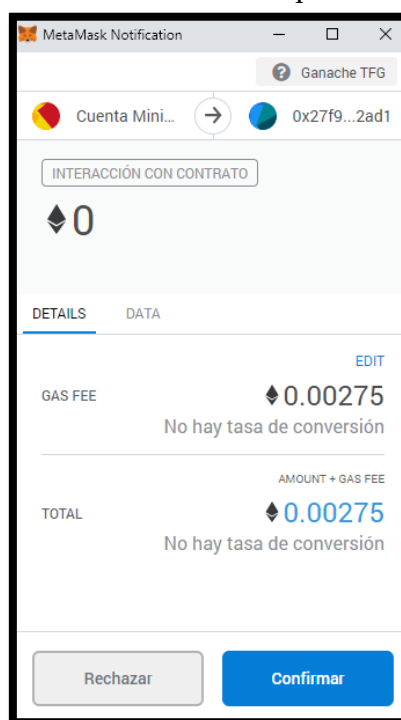


Ilustración 83. Confirmación de transacción del registro de un CMD

A III. 2.2.3 Ejecución de un Testamento

Para la ejecución de un testamento, basta con introducir el DNI de la persona fallecida y una vez que todos los herederos hayan aceptado o renunciado a la herencia podrá ejecutarse el testamento:

1. Introducir el DNI de la persona fallecida y pulsar sobre “Ejecutar Testamento”

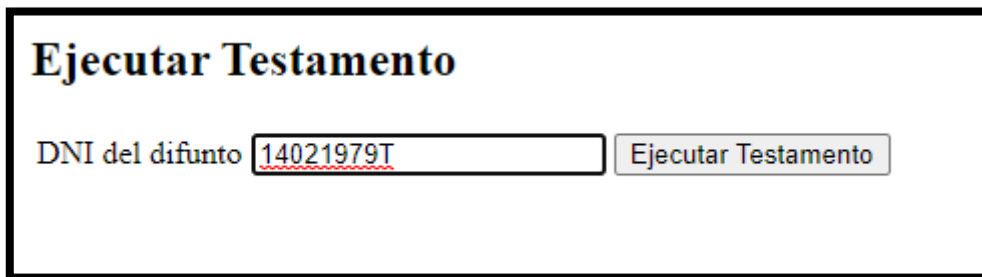


Ilustración 84. Cuadro de ejecución de un Testamento

2. Se abrirá MetaMask para confirmar la transacción

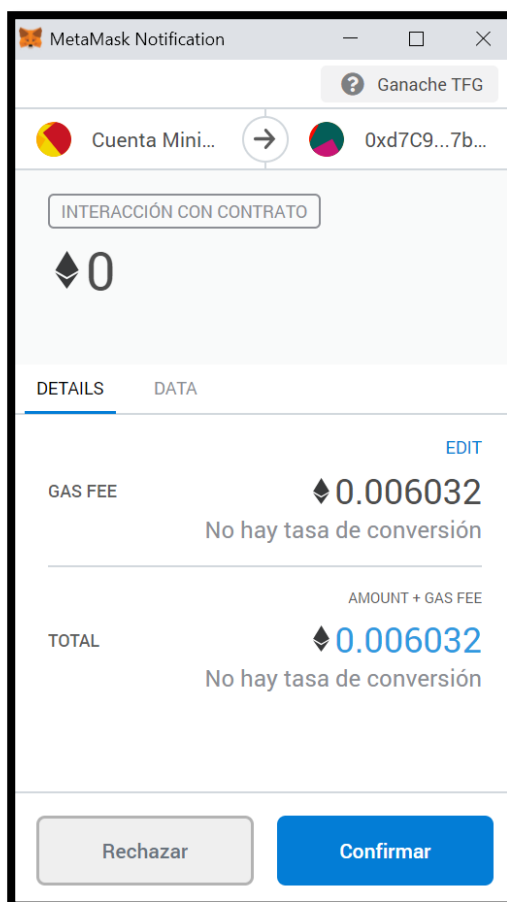


Ilustración 85. Confirmación de transacción de la ejecución de un Testamento

A II. 3 TFG.MITESTAMENTO.COM

En esta sección se detalla el funcionamiento de “tfg.mitestamento.com”. Esta parte de la aplicación el cliente podrá realizar tres acciones: crear un testamento, consultar su Certificado de Últimas Voluntades junto con todos los testamentos incluidos y consultar trámites pendientes para aceptar o renunciar a herencias.

A III. 3.1 CREACIÓN DE TESTAMENTOS

Para realizar la escritura de un testamento:

1. El usuario entra en la URL “tfg-mitestamento.com” con su cuenta en MetaMask activada. Tal y como se explica en A III.1 *Inicio de la aplicación*
2. En la sección “Crear Testamento”, el usuario debe introducir su fecha de nacimiento y pulsar sobre “Comenzar Testamento”.

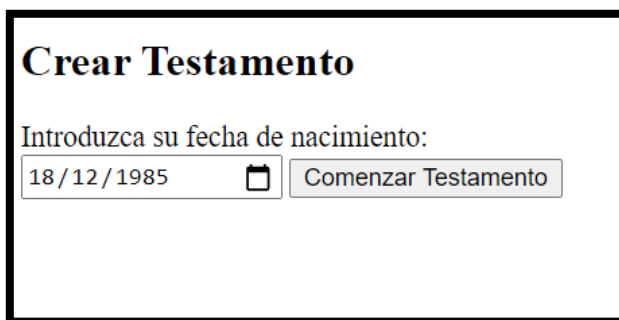


Ilustración 86. Cuadro de inicio de un Testamento

3. Al pulsar “Comenzar Testamento”, se abre MetaMask para confirmar la transacción tal y como se muestra en *Ilustración 87*. Aunque no se ha escrito todavía el testamento, se produce una transacción y por lo tanto una escritura en la red de blockchain de un testamento vacío. Esto es para dejar constancia, en el caso de que haya un fallo o cualquier irregularidad, de la intención de escribir un testamento y, por lo tanto, la intención de testar.

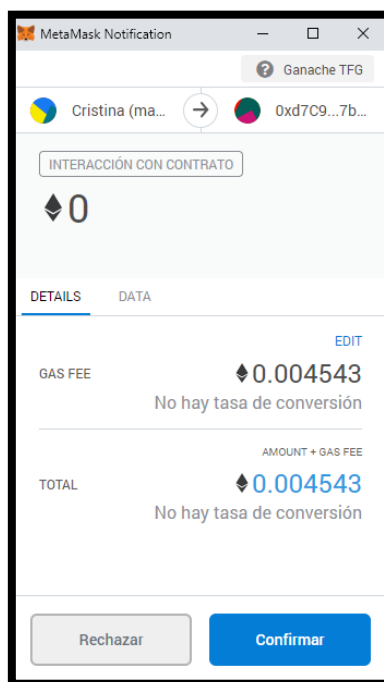


Ilustración 87. Confirmación de transacción de la creación de un Testamento

4. Una vez confirmada la transacción, se despliega en la aplicación un formulario con el id del testamento creado y las fincas del testador para asignar herederos tal y como se muestra en la *Ilustración 88*. Para nombrar herederos, introducir el número de herederos de cada finca y pulsar “Aceptar” en cada uno.

Crear Testamento

Introduzca su fecha de nacimiento:

Testamento creado con
id:99327612663062764484370705614696440997313456685710162459070959038195949484255

1111

Madrid Chalet Porcentaje: 100

Introduzca numero de herederos:

2222

Madrid Piso Porcentaje: 60

Introduzca numero de herederos:

Ilustración 88. Selección del número de herederos

5. Al pulsar “Aceptar”, se desplegará un cuadro para asignar propiedades a cada heredero que se nombre. Rellenamos el cuadro con los DNIs de los Herederos y el porcentaje de la propiedad que se le asigna:

Crear Testamento

Introduzca su fecha de nacimiento:

Testamento creado con
id:99327612663062764484370705614696440997313456685710162459070959038195949484255

1111 Madrid Chalet Porcentaje: 100

Introduzca numero de herederos:

-Propietario (dni) 1 Porcentaje

-Propietario (dni) 2 Porcentaje

2222 Madrid Piso Porcentaje: 60

Introduzca numero de herederos:

-Propietario (dni) 1 Porcentaje

-Propietario (dni) 2 Porcentaje

Ilustración 89. Asignación traspasos en un testamento

6. Una vez rellenado el cuadro, se pulsa sobre “Firmar Testamento” y se abrirá MetaMask para confirmar la Transacción (ver *Ilustración 90*). Al confirmar esta transacción, se rellenará el Testamento creado en los puntos 2 y 3 de A III. 3.1 *Creación de Testamentos*. Por lo que a no ser que no se realicen asignaciones, el testamento no quedará vacío.

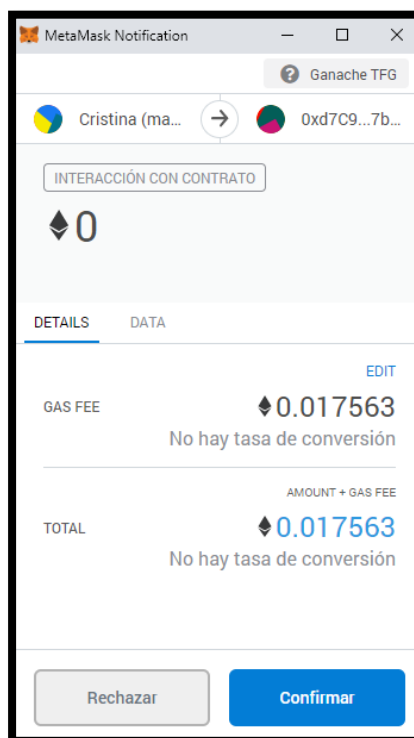


Ilustración 90. Confirmar transacción de firma de un Testamento

A III. 3.2 CONSULTA DEL CERTIFICADO DE ÚLTIMAS VOLUNTADES Y TESTAMENTOS

La consulta de un Certificado de Últimas Voluntades (CUV) permite consultar los Testamentos realizados y el detalle de los traspasos creados en cada testamento. Se visualiza en rojo la información que está almacenada en la BBDD y en negro la información almacenada en la blockchain.

A III. 3.2.1 Consulta de un Certificado de Últimas Voluntades

1. Al entrar en la aplicación, automáticamente se detecta el usuario conectado con MetaMask y se carga el CUV de dicho usuario tal y como se muestra en la *Ilustración 91. Vista de la consulta del CUV de un cliente*

Certificado de Últimas Voluntades:

Id CUV 14153675024247465614100549727091531156561917120150544129442700963158298545024

Nombre de la persona **CRISTINA**

DNI de la persona 18121985C

Cuenta de la persona 0x09Af12DAD9B326B88C84C58b314CA4Fcce838463

Fecha Nacimiento Miércoles 18/12/1985

Testamentos

Testamento nº 1
Testamento nº 2

Id Testamento

Testamento seleccionado:

Id Testamento:

Id CUV:

Cuenta de la persona

Fecha de creación del testamento.

Estado del testamento

Herederos

Cuentas herederos

Decisión de herederos(true/false)

Resumen Traspasos

Ilustración 91. Vista de la consulta del CUV de un cliente

A III. 3.2.2 Consulta de un Testamento

- En el campo “Testamentos” (Verde) del Certificado de Últimas Voluntades, figuran los Testamentos que el cliente ha realizado. Al seleccionar cualquiera de ellos se carga la información de dicho testamento. Véase *Ilustración 92. Consulta de un CUV en detalle*.

A III. 3.2.3 Consulta de un Traspaso

- Debajo de “Resumen Traspasos” figuran todos los traspasos o asignaciones del testamento seleccionado. Para ver en más detalle un traspaso abra el desplegable para seleccionar uno (Azul) y se cargará la información automáticamente. Véase *Ilustración 92. Consulta de un CUV en detalle*.

Certificado de Últimas Voluntades:

Id CUV 14153675024247465614100549727091531156561917120150544129442700963158298545024
Nombre de la persona CRISTINA
DNI de la persona 18121985C
Cuenta de la persona 0x09Af12DAD9B326B88C84C58b314CA4Fcce838463
Fecha Nacimiento Miércoles 18/12/1985
Testamentos Testamento nº 1 ▲
Testamento nº 2 ▼
Id Testamento 99327612663062764484370705614696440997313456685710162459070959038195949484255

Testamento seleccionado:

Id Testamento: 99327612663062764484370705614696440997313456685710162459070959038195949484255
Id CUV: 14153675024247465614100549727091531156561917120150544129442700963158298545024
Cuenta de la persona 0x09Af12DAD9B326B88C84C58b314CA4Fcce838463
Fecha de creación del testamento. Jueves 20/8/2020
Estado del testamento Sin Ejecutar
Herederos LUCIA (dni: 04082003L), PEPE (dni: 13032005P),
Cuentas herederos 0x67D7a0FAffAb5d3bb9D39127bcEAA1F73383F18F,0xCaDDFA8A492CCE8ED160E9194252960a8DBE7cF2
Decisión de herederos(true/false) false,false

Resumen Traspasos

Nº Traspaso	Idufir	Herederos	Porcentajes
1	1111	0x67D7a0FAffAb5d3bb9D39127bcEAA1F73383F18F	50
		0xCaDDFA8A492CCE8ED160E9194252960a8DBE7cF2	50
2	2222	0x67D7a0FAffAb5d3bb9D39127bcEAA1F73383F18F	50
		0xCaDDFA8A492CCE8ED160E9194252960a8DBE7cF2	50

Traspaso nº 2 ▼

Idufir	2222
Propietarios:	LUCIA (dni: 04082003L), PEPE (dni: 13032005P),
Propietarios (Cuentas):	0x67D7a0FAffAb5d3bb9D39127bcEAA1F73383F18F,0xCaDDFA8A492CCE8ED160E9194252960a8DBE7cF2
Porcentajes	50,50
Propietarios rechazan:	
Propietarios rechazan (Cuentas)	
Porcentajes rechazan	
Propietarios aceptados:	
Propietarios aceptados (Cuentas)	
Porcentajes aceptados	

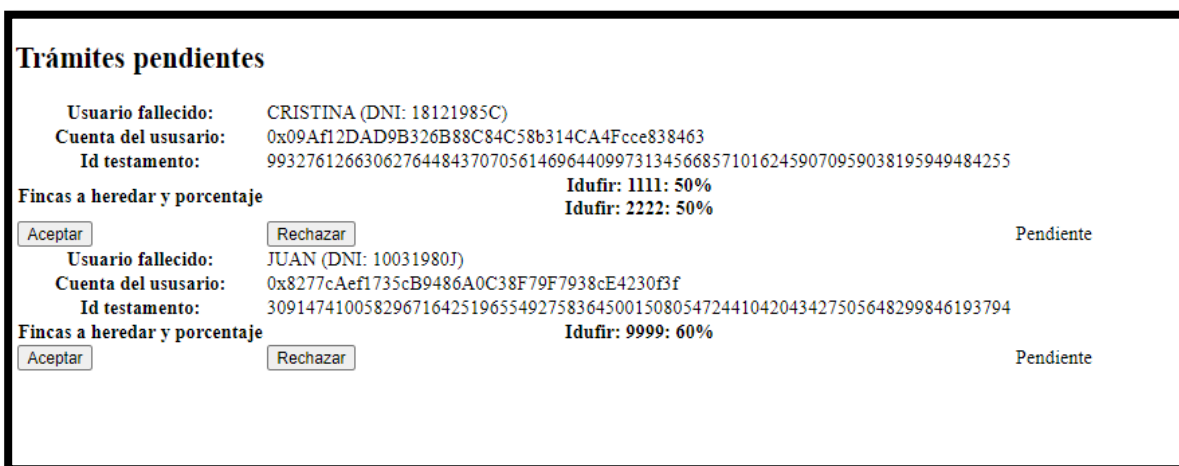
Ilustración 92. Consulta de un CUV en detalle

A III. 3.3 TRÁMITE PENDIENTES

La sección “Trámites pendientes” permite consultar las notificaciones de defunciones en las que el usuario ha sido nombrado heredero. En esta sección el usuario podrá consultar la herencia en las que ha sido nombrado heredero y aceptar/renunciar a dichas herencias.

A III. 3.3.1 Consulta de un Trámite pendiente

- Al entrar en la aplicación, se muestra automáticamente los trámites pendientes con la información necesario sobre el testador y la herencia asignada al usuario.



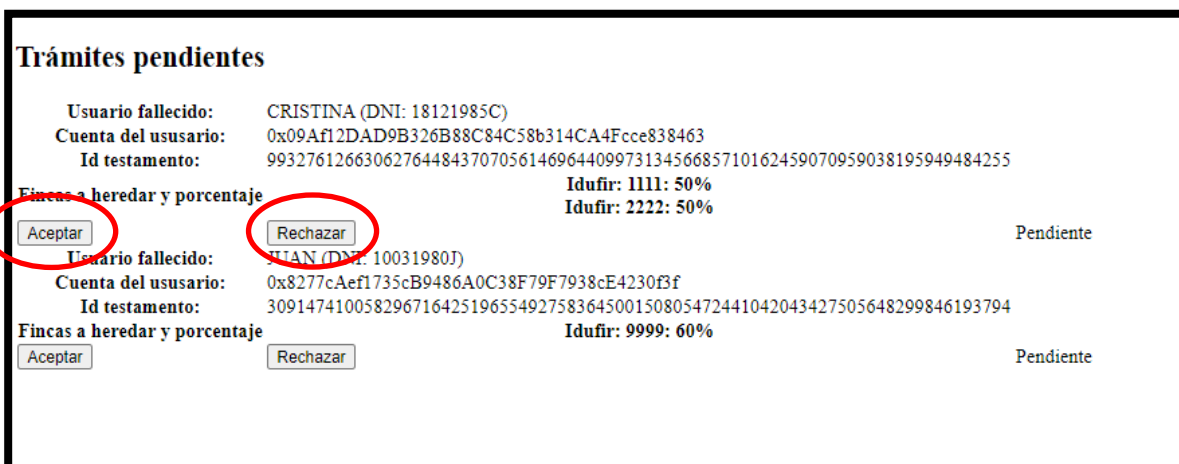
Trámites pendientes

Usuario fallecido: CRISTINA (DNI: 18121985C) Cuenta del usuario: 0x09Af12DAD9B326B88C84C58b314CA4Fcce838463 Id testamento: 99327612663062764484370705614696440997313456685710162459070959038195949484255	Idufir: 1111: 50% Idufir: 2222: 50%	
Fincas a heredar y porcentaje Aceptar Rechazar		Pendiente
Usuario fallecido: JUAN (DNI: 10031980J) Cuenta del usuario: 0x8277cAef1735cB9486A0C38F79F7938cE4230f3f Id testamento: 30914741005829671642519655492758364500150805472441042043427505648299846193794	Idufir: 9999: 60%	
Fincas a heredar y porcentaje Aceptar Rechazar		Pendiente

Ilustración 93. Vista de Trámites pendientes de un usuario

A III. 3.3.2 Aceptar/renunciar a una herencia

- Para aceptar o renunciar a una herencia, basta con pulsar sobre “Aceptar” o “Rechazar” en los botones de cada notificación.



Trámites pendientes

Usuario fallecido: CRISTINA (DNI: 18121985C) Cuenta del usuario: 0x09Af12DAD9B326B88C84C58b314CA4Fcce838463 Id testamento: 99327612663062764484370705614696440997313456685710162459070959038195949484255	Idufir: 1111: 50% Idufir: 2222: 50%	
Fincas a heredar y porcentaje Aceptar Rechazar		Pendiente
Usuario fallecido: JUAN (DNI: 10031980J) Cuenta del usuario: 0x8277cAef1735cB9486A0C38F79F7938cE4230f3f Id testamento: 30914741005829671642519655492758364500150805472441042043427505648299846193794	Idufir: 9999: 60%	
Fincas a heredar y porcentaje Aceptar Rechazar		Pendiente

Ilustración 94. Botones aceptar/rechazar herencia

