GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

BLOCKCHAIN Y SMART CONTRACTS: SERVICIO DE AUTENTICACIÓN DE IDENTIDADES DIGITALES

Autor: Claudia Blanco García

Director: Atilano Ramiro Fernández-Pacheco Sánchez-Migallón

Madrid

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

Blockchain y Smart Contracts: Servicio de Autenticación de Identidades Digitales en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el curso académico 2022/23 es de mi autoría, original e inédito y no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido tomada de otros documentos está debidamente referenciada.

Fdo.: Claudia Blanco García Fecha: 04/Junio/2023

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

71216314B ATILANO RAMIRO FERNÁNDEZ-PACHECO

Firmado digitalmente por 71216314B ATILANO RAMIRO FERNÁNDEZ-PACHECO
Fecha: 2023.06.04 15:32:42 +02'00'

Fdo.: Atilano Ramiro Fernández-Pacheco Sánchez-Migallón Fecha: 04/Junio/2023

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN

TRABAJO FIN DE GRADO

BLOCKCHAIN Y SMART CONTRACTS: SERVICIO DE AUTENTICACIÓN DE IDENTIDADES DIGITALES

Autor: Claudia Blanco García

Director: Atilano Ramiro Fernández-Pacheco Sánchez-Migallón

Madrid

Agradecimientos

Mi más sincero agradecimiento a todos los que me han ayudado a lo largo de esta etapa y este proyecto.

En primer lugar, a mi director, Atilano, por despertar mi interés en la tecnología *Blockchain* a través de sus asignaturas, y por su ayuda y sus consejos en la planificación y organización de este Trabajo de Fin de Grado.

En segundo lugar, a mi familia, mi madre María Jesús, mi padre Raúl y mi hermana Serena, que durante estos cuatro años de carrera me han apoyado y animado a seguir siempre adelante.

También quiero expresar mi agradecimiento a la Universidad Pontificia Comillas (ICAI) por hacerme sentir siempre bienvenida en sus aulas.

A todos ellos, mil gracias.

BLOCKCHAIN Y SMART CONTRACTS: SERVICIO DE AUTENTICACIÓN DE IDENTIDADES DIGITALES

Autor: Blanco García, Claudia.
Director: Fernández-Pacheco Sánchez-Migallón, Atilano Ramiro.
Entidad Colaboradora: ICAI – Universidad Pontificia Comillas

RESUMEN DEL PROYECTO

Este proyecto desarrolla una identidad digital financiera basada en Blockchain que es respaldada por un *rating* crediticio y verificada por diversas organizaciones. Los usuarios pueden utilizarla para solicitar préstamos. Ciertas organizaciones legítimas pueden otorgar puntos positivos o negativos al *rating* de los usuarios según su comportamiento "crediticio".

Palabras clave: *Blockchain*, *Ethereum*, *Smart Contract*, KYC, API

1. Introducción

La autenticación de identidades es crucial en las transacciones económicas actuales. En la actualidad, los datos personales están generalmente centralizados y controlados por entidades gubernamentales o empresas, limitando la libertad de las personas y su acceso a servicios básicos. Además, el crecimiento del Internet de las Cosas y la creación de múltiples identidades en línea por parte de los usuarios ha generado problemas de privacidad y control de datos.

Los procesos de identificación, como el Conoce a tu Cliente o KYC (por sus siglas en inglés, *Know Your Customer*), en el sector financiero, siguen siendo lentos y costosos para las organizaciones. Los datos generados en estos procesos son utilizados por instituciones como las sociedades de información crediticia, que tienen información sobre el historial crediticio de los individuos. Sin embargo, en España estas entidades suelen ofrecer solo información negativa, sin considerar datos positivos que reflejen la capacidad financiera real de las personas.

El proyecto busca mejorar esta situación al proporcionar una identidad digital financiera completa respaldada por *Blockchain*. Esto permite una evaluación más precisa de la capacidad de pago de los individuos, considerando tanto los datos financieros positivos como los negativos. Al proporcionar una identidad verificada en *Blockchain* y basada en un rating crediticio, se facilita el acceso a servicios financieros y se fomenta la inclusión económica.

En resumen, el proyecto se enfoca en mejorar la gestión de identidades financieras digitales, proporcionando seguridad, eficiencia y acceso a servicios financieros a los usuarios a través de una identidad respaldada por *Blockchain* y verificada por diversas organizaciones.

2. Definición del proyecto

El objetivo principal del proyecto es solucionar el problema de la falta de un historial de crédito positivo en España y el poco control sobre ciertos datos personales en las identidades digitales actuales utilizando la tecnología *Blockchain*. Además, el proyecto

busca agilizar los procesos KYC que se usan en ciertas organizaciones para verificar a los clientes con el fin de detectar actividades ilícitas o fraude.

Para cumplir este objetivo se desarrolla una *Dapp* para desplegar un *Smart Contract* que guarde ciertos datos de usuarios y organizaciones en *Blockchain*, para que esta información sea inmutable y segura.

El proyecto engloba tanto el desarrollo de la *Dapp* como la investigación sobre trabajos similares y soluciones de identidades digitales actuales.

3. Descripción del modelo/sistema/herramienta

El funcionamiento del sistema es sencillo. El usuario se registra en la plataforma, para lo que es necesario que proporcione a la plataforma ciertos datos personales. Entre ellos está su número de Documento Nacional de Identidad (DNI), y un PDF oficial del mismo que será verificado a través de una API del Ministerio del Interior español. Una vez registrados sus datos y verificada su identidad, el usuario entra a formar parte del sistema de puntuación o *rating* crediticio. Este *rating* es otorgado al usuario por ciertas organizaciones legítimas del sistema, en general entidades crediticias o financieras, que pueden otorgarle puntos positivos si devuelve un préstamo a tiempo o negativos en caso contrario. El *rating* está guardado en *Blockchain*.

Las organizaciones también pasan por un proceso de verificación al registrarse, con un código de verificación proporcionado por la Asociación Española de Banca (AEB). Además, también pueden puntuarse entre ellas para hacer más fiable el sistema. Además, si tienen más de una cierta puntuación, es decir, si son más fiables que otras, tienen acceso a APIs del Ministerio del Interior, de la Central de Información de Riesgos del Banco de España (CIRBE), de la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y de Hacienda, que les permite obtener más información sobre los usuarios para agilizar los procesos KYC.

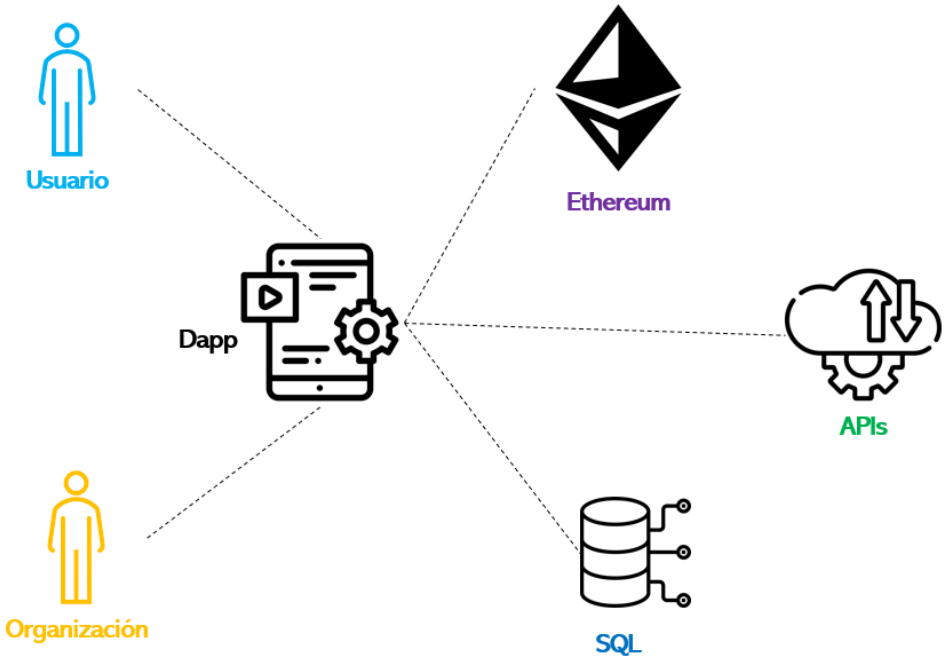


Ilustración 1: Esquema del sistema

Para poder desarrollar estas funcionalidades, ha sido necesario integrar diferentes soluciones de software.

La *Dapp* se ha desarrollado utilizando un *Smart Contract* programado en *Solidity* y desplegado en un nodo *Ethereum* de *Ganache* usando la extensión de *Remix* en *Visual Studio Code*. Se ha empleado la extensión del navegador de *MetaMask* para el acceso a cuentas de la red de *Ethereum* a través de *JavaScript*. Esta parte de *Back End* se ha conectado con el *Front End* de la web en HTML usando las librerías de *Web3.js* a través de *JavaScript*.

JavaScript también se ha utilizado para la comunicación entre la parte frontal de la aplicación y el *framework* de *Spring Boot* usado para las bases de datos SQL y las APIs *mockeadas*.

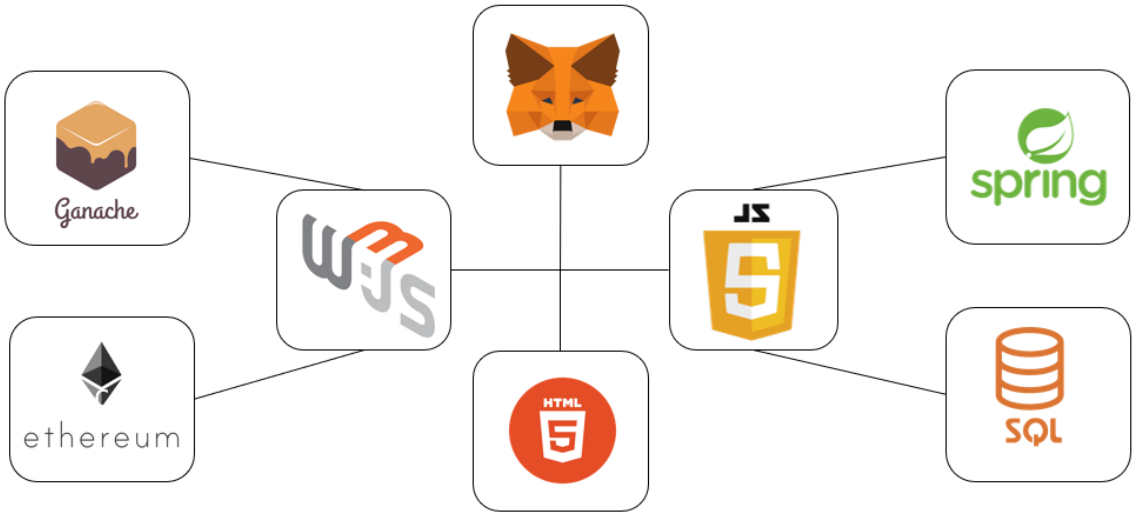


Ilustración 2: Arquitectura del sistema

4. Resultados

Se ha desarrollado con éxito una aplicación web que proporciona a los usuarios una identidad financiera digital basada en un rating guardado en *Blockchain*.

El sistema desarrollado agiliza los procesos KYC tradicionales, posiblemente reduciendo costes temporales y económicos para las entidades crediticias y mejorando la experiencia del cliente. También aumenta la seguridad, la fiabilidad y la transparencia en la verificación de clientes en estos procesos.

Además, este sistema crea un sistema de rating crediticio que incluye datos positivos, proporcionando a los clientes una identidad financiera más completa que la que proporcionan los burós de crédito negativos tradicionales en España.

5. Conclusiones

Este proyecto demuestra cómo las entidades financieras y crediticias pueden disminuir el coste de sus procesos KYC basándose en la tecnología Blockchain. Esta tecnología ha demostrado ser crucial para conseguir un equilibrio entre la necesidad de procesos KYC

ágiles y las preocupaciones por falta de seguridad y privacidad en las identidades digitales en Internet.

La aplicación web desarrollada supone un novedoso punto de partida para una identidad digital financiera más completa, basada en incluso más datos socioeconómicos, además de para la mejora de procesos KYC en diferentes tipos de organizaciones.

6. Referencias

Ondato. (2022). *The real cost of KYC & AML compliance for the financial sector*.

Rodrigues, R. (2015). Competencia Informacional, identidad digital y privacidad de datos: retos y desafíos que nos trae internet hoy. *Repositorio Institucional Universidad Centroamericana*, 3-4.

BLOCKCHAIN AND SMART CONTRACTS: DIGITAL IDENTITY AUTHENTICATION SERVICE

Author: Blanco García, Claudia.
Supervisor: Fernández-Pacheco Sánchez-Migallón, Atilano Ramiro.
Collaborating Entity: ICAI – Universidad Pontificia Comillas

ABSTRACT

This project develops a digital financial identity based on Blockchain that is backed by a credit rating and verified by different organizations. The users can use it to apply for loans. Certain legitimate organizations can grant positive or negative points to the users' ratings according to their "credit" behavior.

Keywords: Blockchain, Ethereum, Smart Contract, KYC, API

1. Introduction

Identity authentication is crucial in current economic transactions. Nowadays, personal data is centralized and controlled by government entities or companies, limiting people's freedom and their access to basic services. Moreover, the growth of the Internet of Things and the creation of multiple online identities have caused privacy and data control problems.

Identification or Know Your Customer (KYC) processes in the financial sector are still slow and costly for organizations. The data generated in these processes is used by institutions such as credit information entities, which possess information about individuals' credit history. However, in Spain, these entities usually only offer negative information, not considering positive data that reflect people's real financial capabilities.

The project aims to improve this situation by providing users with a complete digital financial identity backed by Blockchain. This allows a more precise evaluation of individuals' payment capability, considering both positive and negative financial data. By providing a verified identity based on a credit rating, it facilitates access to financial services and promotes economic inclusion.

In summary, the project focuses on improving the management of digital financial identities, providing security, efficiency, and access to financial services to users through a Blockchain-backed and verified identity by various organizations.

2. Project definition

The main objective of the project is to solve the problem of the lack of a positive credit history in Spain and the limited control over certain personal data in current digital identities using *Blockchain* technology. Additionally, the project aims to streamline the Know Your Customer (KYC) processes used in certain organizations to verify customers in order to detect illicit activities or fraud.

To achieve this objective, a Dapp is developed to deploy a Smart Contract that stores certain user and organization data on the Blockchain, ensuring the immutability and security of this information.

The project encompasses both the development of the Dapp and research on similar works and existing solutions for digital identities.

3. Description of the system

The operation of the system is straightforward. The user registers on the platform, providing certain personal data. This includes their National Identity Document (DNI) number and an official PDF of the document, which is verified through an API from the Spanish Ministry of Interior. Once their data is registered and their identity is verified, the user becomes part of the credit scoring or rating system. This rating is granted to the user by legitimate organizations within the system, typically credit or financial entities, who can assign positive points if the user repays a loan on time, or negative points if not. The rating is stored on the Blockchain.

Organizations also go through a verification process when registering, with a verification code provided by the Spanish Bank Association (AEB). Additionally, they can also rate each other to enhance the reliability of the system. Furthermore, if an organization achieves a certain score, indicating their higher reliability compared to others, they gain access to APIs from the Ministry of Interior, the Central Credit Risk Information System of the Bank of Spain (CIRBE), the National Association of Financial Credit Establishments (ASNEF), and the Tax Agency. This access allows them to obtain more information about users and streamline the KYC processes.

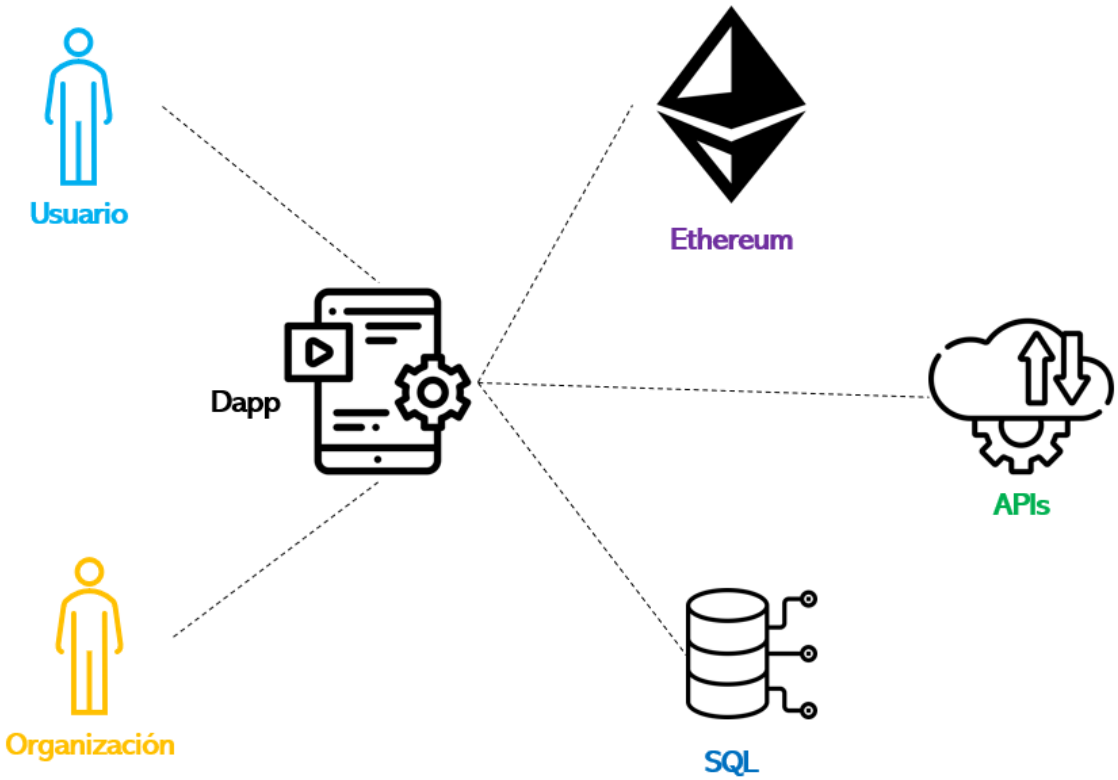


Ilustración 3: System scheme

To implement these functionalities, it was necessary to integrate various software solutions.

The Dapp was developed using a Smart Contract programmed in Solidity and deployed on an Ethereum node of Ganache using the Remix extension in Visual Studio Code. This Back-End component was connected to the HTML Front-End of the web using Web3.js libraries through JavaScript. The MetaMask browser extension has been used for accessing Ethereum accounts through JavaScript.

JavaScript was also used for communication between the front-end of the application and the Spring Boot framework used for SQL databases and mocked APIs.

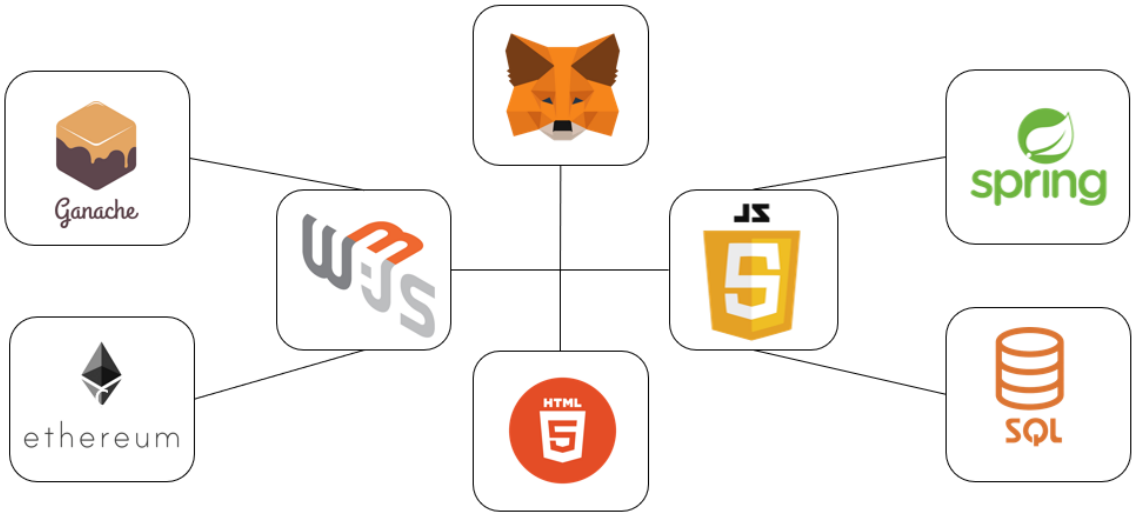


Ilustración 4: System architecture

4. Results

A successful web application has been developed that provides users with a digital financial identity based on a rating stored on the Blockchain.

The developed system streamlines traditional KYC processes, potentially reducing time and cost for credit institutions and improving the customer experience. It also enhances security, reliability, and transparency in customer verification during these processes.

Furthermore, this system creates a credit rating system that includes positive data, providing customers with a more comprehensive financial identity than traditional negative credit bureaus in Spain.

5. Conclusions

This project demonstrates how financial and credit institutions can reduce the cost of their KYC processes by leveraging Blockchain technology. This technology has proven to be crucial in achieving a balance between the need for efficient KYC processes and concerns regarding security and privacy in digital identities online.

The developed web application serves as an innovative starting point for a more comprehensive digital financial identity, incorporating even more socioeconomic data, as well as for the improvement of KYC processes in different types of organizations.

6. References

Ondato. (2022). *The real cost of KYC & AML compliance for the financial sector*.

Rodrigues, R. (2015). Competencia Informacional, identidad digital y privacidad de datos: retos y desafíos que nos trae internet hoy. *Repositorio Institucional Universidad Centroamericana*, 3-4.

Índice de la memoria

Índice de ilustraciones

Índice de fragmentos de código

Índice de tablas

Capítulo 1. INTRODUCCIÓN

La autenticación de identidades es la base de muchas transacciones económicas. En el pasado, estos contratos o acuerdos se llevaban a cabo de forma presencial, pero en la actualidad una gran parte de las transacciones se llevan a cabo digitalmente. En muchos casos, esto requiere una identidad digital, es decir, una forma de identificación o autenticación que hace posible que las entidades identifiquen personas, dispositivos u objetos en el mundo digital. Además, es necesario que la identificación de personas sin un intermediario físico se haga de forma eficiente y segura.

1.1 MOTIVACIÓN DEL PROYECTO

La identidad individual es esencial para el funcionamiento de la sociedad y de la economía. Para las personas, la identidad suele estar compuesta por nombre y apellidos, fecha de nacimiento, nacionalidad, número de la seguridad social… Estos datos suelen estar gestionados por entidades centralizadas, como gobiernos y empresas, y almacenados en bases de datos también centralizadas, en lugar de estar gestionados por los propios dueños de esos datos.

Por otro lado, millones de personas carecen de acceso a una forma de identidad física, lo que les impide reclamar propiedad de su identidad y, por tanto, los emplaza en una situación vulnerable: no pueden votar, abrir una cuenta bancaria, trabajar… Es decir, su libertad se ve limitada. En concreto, muchas personas se encuentran en una situación de libertad financiera limitada.

En los últimos años, el *Internet of Things* (*IoT*) o Internet de las Cosas ha experimentado un crecimiento exponencial en las transacciones, y este aumento se ha intensificado aún más debido a la pandemia de Covid-19. Sin embargo, este crecimiento también ha generado ciertos problemas. En muchos casos, los usuarios carecen de control sobre cómo se utilizan o comparten sus datos personales, ya que estos suelen ser gestionados por entidades

centralizadas, como gobiernos, y almacenados en bases de datos también centralizadas. Esta falta de control plantea preocupaciones en cuanto a la privacidad y la seguridad de los datos en el entorno del IoT.

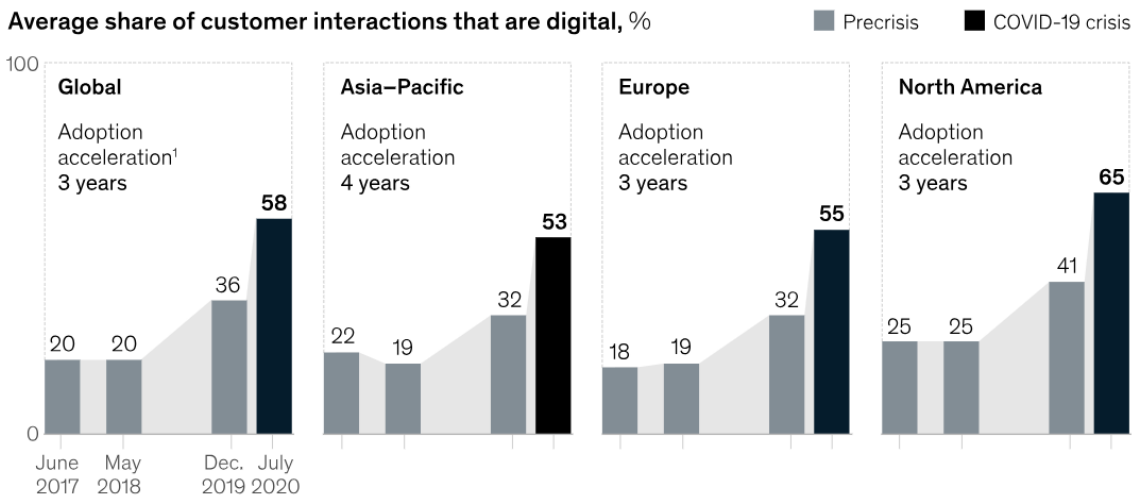


Ilustración 5: Proporción de productos o servicios de diferentes áreas de negocio que están parcial o completamente digitalizados de 2017 a 2018 (McKinsey & Company, 2020)

Por otro lado, los procesos de identificación de clientes en entornos financieros, como los procedimientos *Know Your Customer* (KYC) o Conoce a Tu Cliente, son fundamentales para garantizar la seguridad y prevenir actividades ilícitas como el fraude o el lavado de dinero. Además, estos procesos permiten a las organizaciones conocer mejor a sus clientes y entender sus necesidades financieras, lo que contribuye a establecer relaciones más sólidas y a ofrecer productos y servicios personalizados. La implementación de tecnologías como la inteligencia artificial y el reconocimiento facial ha agilizado el proceso de verificación de identidad, reduciendo los costos y acelerando la toma de decisiones. Sin embargo, a pesar de los avances en la digitalización del mundo de la banca, estos procesos aún presentan desafíos en términos de tiempo y coste para algunas organizaciones.

Uno de los inconvenientes principales es la lentitud en la validación de la información necesaria para la identificación de clientes. Los requisitos de validación de edad, nacionalidad, estudios y solvencia pueden ser procesos laboriosos y consumir mucho tiempo.

Esto puede ralentizar la aprobación de créditos o préstamos y generar frustración tanto para los clientes como para las entidades financieras.

En un proceso KYC tradicional, la recopilación y verificación de los datos de los clientes se realiza de manera presencial, y con documentos en papel.

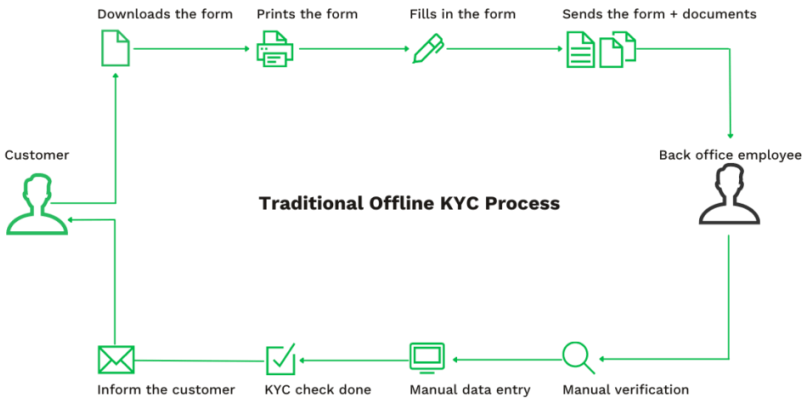


Ilustración 6: Proceso KYC tradicional presencial (Klippa, 2022)

Se trata de un proceso que consume mucho tiempo, tanto para el cliente como para la organización. La digitalización de estos procesos, siguiendo el mismo modelo, solo mejora una parte del proceso para el cliente:

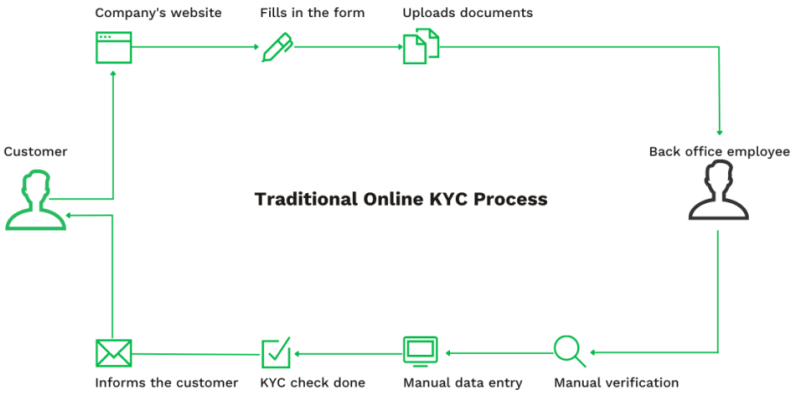


Ilustración 7: Proceso KYC tradicional online (Klippa, 2022)

No solo se trata de procesos lentos, sino que también suponen un mayor riesgo de error al apoyarse en tantas verificaciones manuales y un mayor riesgo de seguridad y privacidad de la información de los clientes.

Algunos de los datos utilizados en los procesos KYC que llevan a cabo organizaciones como bancos o entidades crédito son proporcionados por sociedades de información crediticia, que recopilan la información de ciudadanos que tienen algún tipo de crédito vigente. Estas entidades también se denominan burós de crédito. En muchos países, como Estados Unidos o Australia, estos burós son de crédito positivo y negativo, y se centran en lo que se conoce como *credit score* (puntuación de crédito). En países hispanohablantes solo existen burós de crédito negativos, como la Central de Información de Riesgos del Banco de España (CIRBE).

Los datos negativos de crédito facilitan una información a las entidades bancarias y de crédito sobre la incapacidad previa de saldar una deuda o sobre la insolvencia (temporal o de otro modo) de una persona o empresa en concreto. Por otro lado, los datos positivos financieros aportan una información más precisa y completa de la situación financiera y las capacidades de una persona o empresa: límites de tarjetas de crédito y pago de saldos mensuales; pagos a proveedores o acreedores; amortización de capitales; disposición de dinero en efectivo; ingresos habituales o extraordinarios…

Por tanto, los datos negativos solo informan sobre impagos o retrasos en los pagos, pero no indican el número de tarjetas de crédito que tiene, los pagarés que ofrece como medio de pago en lugar de pagar en efectivo, ni de la capacidad financiera real: Si una persona tiene tres tarjetas de crédito, una hipoteca y un crédito personal (o una empresa tiene varios proveedores) y lo paga todo a tiempo, no figurarán datos negativos, con lo cual la información no será completa. Mientras que si se informa de todas estas líneas de crédito (tarjetas e hipotecas en el caso de una persona física y pagos a proveedores en el caso de una empresa) que tiene abiertas, será más evidente su alta capacidad de afrontar sus deudas.

1.2 SOLUCIÓN PROPUESTA

Como se ha explicado, la identificación de clientes en los procesos KYC en el ámbito financiero desempeña un papel crucial para garantizar la seguridad y prevenir el fraude. La necesidad de llevar a cabo estos procesos se encuentra con dificultades al tratarse de procesos tan laboriosos y que requieren tanto tiempo para los clientes y las entidades financieras. El crecimiento del IoT y la digitalización del mundo de la banca han mejorado la eficiencia y la accesibilidad de estos procesos de identificación, pero aún existen muchos obstáculos a superar.

Con el fin de crear una forma de identidad crediticia digital personal, segura y descentralizada sobre la cual el usuario tenga control, se propone desarrollar una aplicación descentralizada (*Dapp*) basada en *Smart Contracts* a través de la cual los usuarios puedan crear su identidad personal y financiera digital, y las organizaciones puedan verificar la identidad y la puntuación de crédito de los usuarios.

Se propone por tanto un sistema de identificación más automatizado que evite los principales costes temporales y económicos de los procesos KYC que las entidades bancarias realizan sobre sus clientes. Con este objetivo, el proyecto se lleva cabo utilizando *Smart Contracts* (Contratos Inteligentes), programas informáticos que ejecutan automáticamente acuerdos y transacciones sin intermediarios. También se hace uso de APIs, interfaces de programación de aplicaciones, que permiten a las organizaciones obtener información adicional sobre sus clientes de manera automática y sencilla. Además, la *Dapp* proporcionará a las organizaciones que la utilicen una mayor comodidad y seguridad al poder utilizar una *wallet* de *MetaMask* que almacene sus claves criptográficas.

Por otro lado, la *Dapp* proporcionará a los clientes mayor eficiencia en su identificación a la hora de solicitar préstamos o créditos, además de una identidad personal que les dará una mayor libertad financiera.

Por tanto, la meta de este proyecto es crear una identidad financiera digital respaldada por datos socioeconómicos basada en *Smart Contracts* que mejore la eficiencia y la transparencia de los procesos KYC realizados por entidades financieras.

Capítulo 2. DESCRIPCIÓN DE LAS TECNOLOGÍAS

En este capítulo se describen las tecnologías utilizadas para el desarrollo del proyecto. Posteriormente, en el Capítulo 5, se describirá más en detalle la arquitectura del sistema y la integración de las tecnologías utilizadas.

2.1 ETHEREUM

Bitcoin fue la primera moneda digital descentralizada, lanzada en 2009. La plataforma *Ethereum*, fundada por Vitarik Buterin y lanzada en 2015, surgió para ampliar la funcionalidad de *Bitcoin* como una plataforma universal basada en *Blockchain* para la ejecución de *Smart Contracts* (contratos inteligentes). La criptomoneda de esta plataforma es el *Ether* (ETH).

Aunque *Bitcoin* y *Ethereum* tienen ciertas características comunes, se ha elegido usar *Ethereum* porque ofrece algunas ventajas frente a *Bitcoin*. Para empezar, el tiempo de las transacciones con *Ethers* es más rápido que con *Bitcoins*, y la recompensa por minería es mayor. Además, no existe límite de *Ethers*, a diferencia de *Bitcoins*, y los *Smart Contracts* están integrados directamente en la plataforma, por lo que no se necesita ningún software externo. Por otro lado, existen muchas redes de *Ethereum*, y algunas son redes de prueba que permiten hacer simulaciones. Esto se explicará más en detalle en el Ganache.

Ethereum puede definirse como una máquina de estados. Los nodos de la red de *Ethereum* ven el estado global de la máquina. Un usuario puede interactuar con la red emitiendo transacciones, que representan una transición de estado. Los nodos de la red eligen transacciones del conjunto de transacciones no confirmadas, verifican su validez, realizan los cálculos correspondientes y actualizan el estado de la red. Hay dos tipos de cuentas en *Ethereum*: cuentas controladas por una clave privada y cuentas controladas por un *Smart Contract*, un código desplegado en la *Blockchain*.

Ethereum es una red *peer-to-peer* en la que los nodos o *peers* tienen el poder: la red no depende de un agente externo, ya que la información de las transacciones se almacena de forma encriptada y segura.

Ilustración 8: Ethereum

En esta red *peer-to-peer* se habla de mecanismos de consenso, algoritmos de consenso utilizados en *Blockchain* para alcanzar acuerdos sobre el estado de la red y validar las transacciones (Ethereum, 2023). Se pueden definir como mecanismos de consenso, o más bien como bases para estos, algunos como *Proof of Work*, *Proof of Stake* y *Proof of Authority*. *Proof of Stake* (PoS) es el mecanismo de consenso que utiliza *Ethereum* para validar y confirmar transacciones en la actualidad. A diferencia del *Proof of Work* (PoW), que era el algoritmo utilizado en la red Ethereum hasta 2022, PoS no se basa en la potencia de cálculo computacional, sino en la tenencia de criptomonedas.

En lugar de mineros como anteriormente, *Ethereum* ahora cuenta con validadores. Estos validadores son participantes de la red que bloquean una cierta cantidad de *Ether* como garantía y están dispuestos a confirmar transacciones. La selección de los validadores para crear un bloque se realiza en función de la cantidad de *Ether* que han bloqueado. Esto significa que aquellos con más *Ether* tienen más posibilidades de ser seleccionados para validar transacciones y recibir recompensas.

El PoS introduce un concepto llamado "castigo" (*slashing*), que tiene como objetivo desincentivar el comportamiento malicioso o deshonesto de los validadores. Si un validador actúa de manera perjudicial para la red, como intentar validar bloques inválidos o dobles gastos, puede perder parte o la totalidad de su garantía.

Una de las principales ventajas de PoS en *Ethereum* es su capacidad para escalar de manera más eficiente. A medida que aumenta el número de validadores en la red, se pueden procesar más transacciones simultáneamente, lo que mejora la velocidad y la capacidad de la red en general.

Además, PoS promueve la participación de los poseedores de *Ether* a largo plazo en el mantenimiento y la seguridad de la red. Los usuarios que no tienen el conocimiento técnico o los recursos para realizar la minería PoW tradicional pueden participar en el PoS simplemente bloqueando su *Ether* y convirtiéndose en validadores. Esto democratiza la participación en la red y reduce la centralización de poder en manos de unos pocos.

2.2 SOLIDITY

Solidity es el lenguaje de programación desarrollado para ejecutar los *Smart Contracts*. Se trata de un lenguaje de alto nivel y orientado a objetos, diseñado para interactuar con la *Ethereum Virtual Machine* (EVM). Es similar a otros lenguajes como *C++*, *Python* o *JavaScript*.

Solidity tiene un compilador que lanza el fichero ABI (*Application Binary Interface*) que es un estándar para interactuar con *Smart Contracts* en el entorno de Ethereum. Esto incluye interacciones entre contratos y desde fuera de la *Blockchain*. En este proyecto, el ABI se ha utilizado para interactuar con el *Smart Contract* desde el código de *JavaScript* de una aplicación web basada en *Spring Boot*. Esto se explicará más en detalle en el Entorno de desarrollo.

Algunas de las ventajas de utilizar *Solidity* son:

- Comunidad activa y amplia adopción. *Solidity* es uno de los lenguajes de programación más populares y ampliamente utilizados para *Smart Contracts*. Esto implica una gran cantidad recursos disponibles.
- *Smart Contracts* flexibles y potentes. *Solidity* permite la creación de *Smart Contracts* complejos y sofisticados con funcionalidades avanzadas como herencia, bibliotecas y tipos de datos personalizados, lo que permite la construcción de aplicaciones descentralizadas (*Dapps*) más sofisticadas.
- Integración con Ethereum. Solidity es el lenguaje de programación principal utilizado en *Ethereum*, la plataforma *Blockchain* más grande y establecida. Esto garantiza una alta compatibilidad y facilidad de integración con otras herramientas y protocolos en el ecosistema.

No obstante, también es importante señalar algunas de las desventajas de este lenguaje de programación:

- Seguridad y errores de programación. Debido a la naturaleza irreversible de los contratos inteligentes, los errores de programación en *Solidity* pueden tener consecuencias graves y potencialmente resultar en pérdida de fondos. La seguridad y la auditoría cuidadosa son fundamentales al desarrollar en *Solidity*.
- Evolución y cambios en el lenguaje. *Solidity* está en constante evolución, y nuevas versiones y cambios en el lenguaje pueden requerir actualizaciones y modificaciones en los contratos existentes. Esto puede requerir un mantenimiento continuo y adaptación a las nuevas versiones.

Ilustración 9: Solidity

2.3 GANACHE

Ganache es un entorno que simula la red de *Ethereum* y permite interactuar con *Smart Contracts* en una *Blockchain* privada. Se ha utilizado *Ganache* para crear diferentes cuentas, indicar sus saldos iniciales, ver sus claves privadas y ver las transacciones realizadas, entre otras cosas.

Ilustración 10: Ganache

Se ha utilizado la aplicación de escritorio de *Ganache*, lo que ha permitido crear una red a la que conectar el *Smart Contract* y trabajar con las cuentas de forma más visual y sencilla.

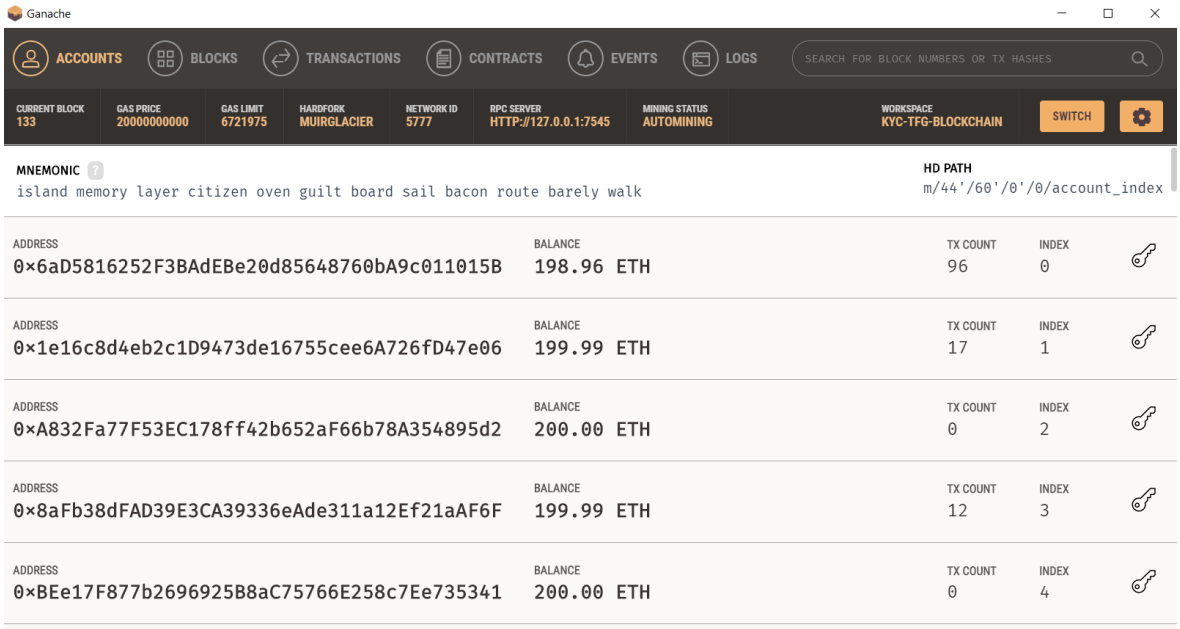


Ilustración 11: Interfaz de la aplicación Ganache

2.4 METAMASK

MetaMask es una *wallet* o cartera de criptomonedas que se ha utilizado en el desarrollo del proyecto para interactuar con la aplicación descentralizada o *Dapp*. En concreto, esta *wallet* tiene una extensión en el navegador web que se ha empleado para conectar las cuentas (*accounts*) de la red de *Ethereum* con la parte frontal de la aplicación. De este modo se ha podido simular la realización de ciertas acciones o funcionalidades de la aplicación por parte de organizaciones diferentes.

Ilustración 12: MetaMask

2.5 FRONT DE LA APLICACIÓN

La aplicación utiliza HTML (*HyperText Markup Language*) y CSS (*Cascading Style Sheets*) como *Front End*, con varios ficheros de código *JavaScript*.

HTML es el lenguaje estándar para establecer la estructura y el contenido de una página web. CSS es un lenguaje de estilo utilizado para describir la apariencia de un documento HMTL.

Es decir, mientras que HTML se enfoca en la estructura y el significado de los elementos de una página web, CSS se ocupa de la presentación de los mismos, como el color, el tamaño, la disposición y otros aspectos visuales.

Ilustración 13: HTML

2.6 ENTORNO DE DESARROLLO

Se ha utilizado *Visual Studio Code* como entorno de desarrollo, principalmente para la aplicación de *Java* y los ficheros web. Se ha instalado *Remix IDE* en este entorno de desarrollo. En concreto se ha instalado la extensión *Ethereum Remix*.

2.6.1 REMIX IDE

Remix IDE es una interfaz que permite editar y compilar *Smart Contracts*, y facilita interactuar con la red de Ethereum proporcionando "accesos directos" a la compilación y ejecución de los contratos.

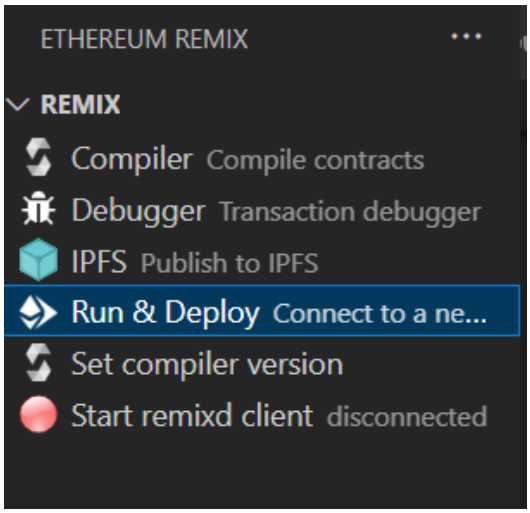


Ilustración 14: Funcionalidades de Ethereum Remix

Se ha usado la interfaz de *Remix* en *Visual Studio Code* para conectar el *Smart Contract* a la red de *Ganache*.

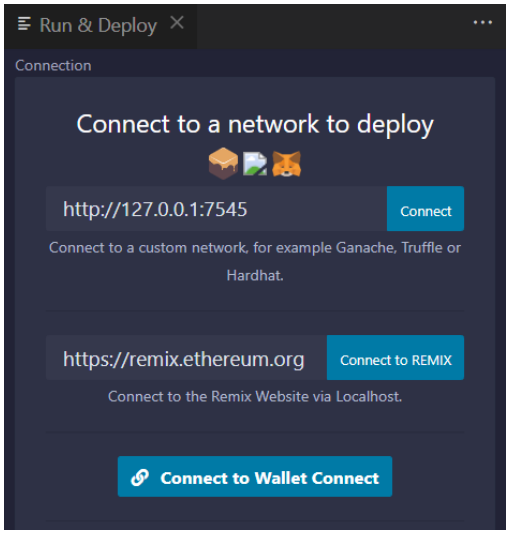


Ilustración 15: Funcionalidades de Ethereum Remix (parte 2)

2.6.2 SPRING BOOT

Spring Boot es un marco de desarrollo de código abierto que facilita el desarrollo de aplicaciones web y microservicios. Proporciona una configuración automática de la estructura de la aplicación a través de la inyección de dependencias.
Algunas de las dependencias que se han utilizado son:

- **Spring-boot-starter-web**. Proporciona las funcionalidades necesarias para crear controladores web y manejar solicitudes HTTP.
- **Lombok**. Ayuda a reducir el código repetitivo en clases de *Java*, generando automáticamente *getters*, *setters* y otros métodos comunes en tiempo de compilación.
- **Spring-boot-starter-jdbc**. Proporciona soporte para acceder a una base de datos relacional utilizando JDBC (*Java Database Connectivity*).
- **H2**. Agrega una base de datos embebida en memoria a la aplicación. H2 es un tipo de base de datos relacional ligera y fácil de usar, que es muy útil para el desarrollo y para hacer pruebas.
- **Org-web3j-core**. Permite la integración con *Ethereum* y *Blockchain*.

2.6.3 WEB3.JS

Web3.js es un conjunto de librerías que permiten interactuar con un nodo local o remoto de *Ethereum* desde un código de *JavaScript*.

Ilustración 16: web3.js

Capítulo 3. ESTADO DE LA CUESTIÓN

3.1 LAS IDENTIDADES DIGITALES

El desarrollo de las identidades digitales ha evolucionado a lo largo del tiempo, pasando por diferentes etapas.

La primera etapa fue la identidad digital centralizada, que surgió con el nacimiento de Internet (Bai, y otros, 2022). En este enfoque, entidades como la IANA (*Internet Associated Numbers Authority*) y la ICANN (*Internet Corporation for Assigned Names and Numbers*) desempeñan un papel importante en la validación y asignación de direcciones IP y nombres de dominio. Sin embargo, esta forma de identidad digital centralizada presenta ciertas limitaciones. La gran cantidad de usuarios en Internet dificulta la validación y gestión de identidades de manera eficiente. Además, al estar controladas por entidades o autoridades externas, existe un mayor riesgo de filtrado de información personal y falta de control por parte de los propios usuarios.

Para abordar algunas de estas limitaciones, se introdujo la identidad digital federada. Este enfoque permite a los individuos utilizar una única identificación personal para acceder e identificarse en diferentes sitios web y servicios. En lugar de depender de una autoridad central, se establece una federación de proveedores de identidad que colaboran entre sí para verificar y autenticar la identidad de los usuarios. Esto proporciona una mayor conveniencia para los usuarios al permitirles utilizar una única identidad en múltiples plataformas y reducir la necesidad de crear y gestionar múltiples cuentas. Sin embargo, aún se requiere cierta confianza en los proveedores de identidad y existen desafíos relacionados con la interoperabilidad y la seguridad de la federación de identidades.

Existe otro modelo de identidad conocido como identidad usuario-céntrica (*user-centric identity*), que coloca al usuario en el centro del proceso de creación de una identidad en línea. Este enfoque ha dado lugar al desarrollo de OpenID, un estándar descentralizado de

identificación digital que permite a los usuarios autenticarse en sitios web y controlar los datos personales que se comparten en dichos sitios. Aunque este modelo proporciona a los usuarios un mayor control sobre sus datos e identidad, muchos optan por registrar su OpenID en un proveedor de servicios público, lo que en realidad implica que su identidad sigue siendo controlada por ese proveedor.

En último lugar, surge el concepto de Identidad Autogestionada o *Self-Sovereign Identity* (SSI). Con SSI, los usuarios tienen el control total sobre su identidad y, además, se descentraliza la recopilación, almacenamiento y uso de datos en el sistema. Para que una identidad sea realmente autogestionada, debe ser validada a través de un sistema de "confianza descentralizada" (decentralized trust) que no esté controlado ni sea propiedad de ninguna organización en particular. Esto implica que otros usuarios pueden verificar la identidad de una persona a través de declaraciones o afirmaciones. La tecnología *Blockchain*, que surgió a partir del artículo "*Bitcoin: A Peer-to-Peer Electronic Cash System*" escrito por Nakamoto en 2008, proporciona la base para este tipo de identidad digital.

Con la arquitectura de SSI, surge el concepto de Identificador Descentralizado (*Decentralized Identifier* o DID). Un DID es un identificador pseudo-anónimo para una persona, empresa u objeto, entre otros. Cada DID está protegido por una clave privada, y solo el propietario de esa clave privada puede demostrar que controla o es dueño de su identidad. Una persona puede tener múltiples DIDs, por ejemplo, uno asociado a una plataforma de juegos y otro asociado a su plataforma bancaria. Esto permite un enfoque más granular y específico en la gestión de la identidad en diferentes contextos y servicios en línea.

Existen algunas aplicaciones que facilitan el proceso de identificación al usuario. En 2019 Microsoft lanzó su propia implementación de DID, ION, una red pública de identificación descentralizada que se ejecuta en la red de *Blockchain* de Bitcoin, aunque evitando los problemas de rendimiento de esta. También en 2019, *WeBank* presentó *WeIdentity*, que asegura la credibilidad y la seguridad en el intercambio de datos, usando el Consortium *Blockchain* como centro de conexión para cada rol de usuario y como depósito de

información, y basándose en los servicios de *Know Your Customer* proporcionados por autoridades. *Sovrin* es un servicio público cuyo objetivo es proporcionar una red en la que cualquiera pueda subir un certificado que contenga una firma digital y que otros usuarios puedan verificarlo. Está basado en SSI.

También existen aplicaciones de identificación digital que no están basadas en *Blockchain*. Un ejemplo es *Australian Keypass Digital iD*, que permite a sus usuarios llevar su identificación digital en una aplicación móvil con la que pueden demostrar su mayoría de edad, entre otras cosas.

3.2 LOS BURÓS POSITIVOS Y NEGATIVOS DE CRÉDITO

En España, el sistema crediticio se basa en la Central de Información de Riesgos del Banco de España (CIRBE), que es un registro de información de riesgos crediticios que recopila datos de todas las entidades financieras del país. Esta información se utiliza para evaluar la solvencia de los clientes y determinar su capacidad para obtener créditos. El registro incluye información sobre préstamos, créditos, avales y garantías bancarias, y está disponible para las entidades financieras, pero no para el público en general. Además, existen empresas de información crediticia que recopilan información sobre el historial crediticio de los ciudadanos, como ASNEF o RAI, que registran a los deudores y su situación de pago. Estas empresas no conceden ni deniegan créditos, sino que proporcionan información que las entidades financieras pueden utilizar para evaluar el riesgo crediticio de los solicitantes de préstamos o créditos.

No obstante, las entidades financieras que acceden a esta información se centran en los datos financieros negativos. De hecho, estas fuentes de información financiera no incluyen datos positivos de forma explícita. Por ejemplo, el fichero ASNEF solo incluye a individuos que han incumplido algún tipo de acuerdo de crédito o pago, pero no tiene información sobre cumplimiento de deudas. Por tanto, las personas o empresas que poseen un historial financiero positivo no pueden beneficiarse de estos sistemas. Es decir, su historial positivo no les proporciona ningún tipo de facilidad directa a la hora de pedir un préstamo o un

crédito, por ejemplo. Queda todo en manos del banco o la entidad crediticia, que utilizará su propio sistema de *scoring* para determinar si aprobarlo o no.

Esto ha dado lugar al aumento de la popularidad de plataformas de pago en cuotas, como *Clearpay* (originalmente *Afterpay*) o *Klarna*, que permiten a sus usuarios obtener "préstamos" de forma sencilla. Estas plataformas de pago en cuotas, o BNPL (por sus siglas en inglés, *Buy Now Pay Later*, Compra Ahora Paga Después), representaron un 8.1% del gasto en compras en línea de consumidores europeos en 2021 (Worldpay, 2022). Según Worldpay (2022), en España, las plataformas BNPL están en auge desde 2021, y se espera que los pagos a través de estos sistemas crezcan un 19,8% anualmente (Research and Markets, 2023). Esto demuestra que hay un mercado para clientes que necesitan pedir préstamos de manera más sencilla, rápida y accesible.

Al utilizar burós positivos y no solo negativos, las instituciones financieras tendrían acceso a un historial de pagos puntuales, cumplimiento de obligaciones y buen comportamiento financiero de los clientes. Esto permitiría a las entidades crediticias o a los prestamistas identificar a los individuos que han demostrado ser más responsables y han tenido un buen comportamiento crediticio a lo largo del tiempo. De este modo podrían ajustar los términos del préstamo de manera más precisa y otorgar tasas de interés más favorables a aquellos clientes.

Además, el cálculo del *spread* de crédito utilizando información financiera positiva reflejaría de manera más justa el nivel de riesgo asociado a cada individuo. El *spread* de crédito se refiere a la diferencia entre la tasa de interés de un préstamo o instrumento de deuda y la tasa de interés considerada libre de riesgo. Es un indicador utilizado en el ámbito financiero para evaluar el nivel de riesgo crediticio asociado a un determinado préstamo o emisor de deuda. En general, cuanto mayor sea el *spread* de crédito, mayor será el riesgo percibido por los prestamistas. Un *spread* de crédito amplio indica que el emisor o prestatario es considerado de mayor riesgo y, por lo tanto, requerirá una mayor compensación en forma de una tasa de interés más alta para atraer a los prestamistas. Por otro lado, un *spread* de crédito estrecho indica que el emisor o prestatario es considerado menos riesgoso, lo que se traduce en una

tasa de interés más baja, ya que los prestamistas están dispuestos a aceptar un menor retorno debido a la mayor confianza en la capacidad de pago del emisor.

Tener en cuenta el historial financiero o crediticio de los clientes a la hora de calcular el *spread* implicaría que los clientes con un historial crediticio sólido y positivo podrían obtener mejores condiciones de préstamo que aquellos con un historial más incierto o negativo, que verían esta incertidumbre reflejada en tasas de interés más altas. Esto fomentaría la responsabilidad financiera y la gestión adecuada de las obligaciones crediticias, incluso en un entorno de altos tipos de interés.

3.3 PROCESOS KYC EN DIFERENTES ORGANIZACIONES

Un proceso KYC (Conoce a Tu Cliente, por sus siglas en inglés) es un conjunto de procedimientos que ciertas empresas y organizaciones implementan para identificar a sus clientes y validar su identidad. Este proceso es especialmente relevante en sectores como las entidades bancarias y crediticias, el ámbito de las telecomunicaciones y las compañías de seguros, donde la confianza y la seguridad son fundamentales.

Las entidades bancarias y crediticias llevan a cabo el KYC como parte de su proceso de apertura de cuentas y servicios financieros. El objetivo principal de este proceso es asegurarse de que sus clientes no estén involucrados en actividades ilegales y evaluar su nivel de riesgo. Estas organizaciones recopilan información personal, como documentos de identificación, comprobantes de domicilio y detalles financieros. Además, realizan controles adicionales, como verificaciones de antecedentes y monitoreo continuo de transacciones, para garantizar el cumplimiento normativo y prevenir el lavado de dinero y la financiación del terrorismo.

Las compañías de telecomunicaciones también requieren llevar a cabo procesos KYC para verificar la identidad de los usuarios sus servicios, como líneas telefónicas móviles o servicios de Internet. Esto ayuda a prevenir el fraude y asegurar que los servicios sean utilizados por personas legítimas. El KYC en este tipo de empresas generalmente implica la

presentación de documentos de identificación y la verificación de información personal. Los procesos KYC en empresas de telecomunicaciones son especialmente relevantes en la actualidad, ya que muchos de los servicios bancarios se han digitalizado. La gran mayoría de los bancos españoles cuentan con una aplicación móvil, y el 86% de los usuarios españoles utiliza aplicaciones de banca tradicional (Applicantes, 2023).

Las compañías de seguros también utilizan procesos KYC para identificar y verificar a los asegurados. Esto implica la recolección de información personal, como datos de identificación y antecedentes médicos, para evaluar el riesgo asociado con la cobertura de seguros solicitada.

Es importante destacar que el proceso KYC no se limita solo a la identificación inicial de los clientes, sino que también implica el monitoreo continuo de las actividades de los mismos a lo largo del tiempo. Esto garantiza que cualquier cambio en las circunstancias o comportamientos de los clientes sea detectado y evaluado en términos de cumplimiento normativo y riesgo.

Sin embargo, este proceso no está exento de desafíos. Es un procedimiento continuo y costoso, tanto en términos de tiempo como económicos, ya que requiere recursos para la recolección y verificación de la información, así como para el monitoreo constante de las actividades de los clientes. Además, la gestión de grandes volúmenes de datos personales requiere un enfoque cuidadoso en cuanto a la privacidad y la seguridad de la información. Como se mencionó anteriormente, los procesos KYC tradicionales implican cierto tratado manual de la información, por lo que la privacidad de los datos de los clientes puede suponer un problema.

En resumen, el proceso KYC es fundamental en diversas industrias para garantizar la confianza, prevenir el fraude y cumplir con los requisitos normativos. A medida que avanza la digitalización, se espera que los procesos KYC continúen evolucionando para adaptarse a los cambios en las tecnologías y las necesidades de seguridad de las organizaciones y los clientes. Muchas empresas llevan a cabo sus procesos de identificación de clientes utilizando técnicas digitales, y el uso de inteligencia artificial y algoritmos de aprendizaje automático

o *Machine Learning* está en auge (Klippa, 2022). Sin embargo, aún quedan problemas por resolver.

3.4 SOLUCIONES KYC ACTUALES

Por otro lado, se han llevado a cabo otros proyectos y trabajos de investigación que abordan una identidad digital para procesos KYC.

Un ejemplo es un trabajo de investigación realizado en la Universidad de Atenas en 2020, en el que se desarrolló un sistema a través del cual los usuarios pueden registrarse y subir sus documentos KYC para que un administrador los verifique y apruebe utilizando un *Smart Contract* público (Kapsoulis, y otros, 2020). Otros proyectos de investigación desarrollan sistemas similares.

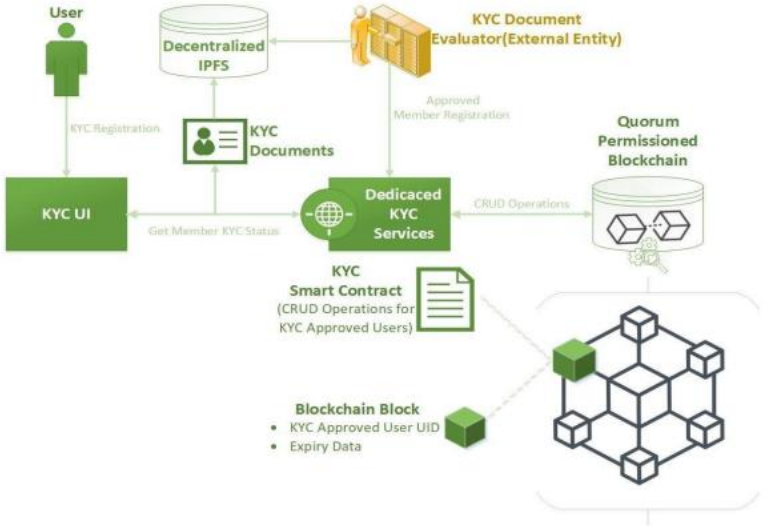


Ilustración 17: Propuesta de KYC basado en Blockchain (Kapsoulis, y otros, 2020)

El IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) publicó en 2019 un artículo describiendo un sistema descentralizado de gestión de transacciones y de derechos de autor basado en *Blockchain* (Zhang & Yin, 2019). Existe un proyecto de investigación reciente que propone un sistema KYC para procesos de *onboarding* de clientes en organizaciones usando *Blockchain* y tecnología IPFS (Singhal, Sharma, Samant, Goswami, & Abhilash,

2020). También existen algunos proyectos de código abierto u *Opensource* en GitHub que incluyen una base para un sistema de identidades descentralizado.

Aunque existen varios proyectos y trabajos de investigación relacionados con la identidad digital y los procesos KYC, es importante destacar que la mayoría de ellos se han desarrollado fuera de España, e incluso fuera de Europa. Además, muchos de estos proyectos son de naturaleza académica y divulgativa, centrándose en la exploración de conceptos y en la presentación de propuestas teóricas.

Además, se debe resaltar que, hasta el momento, no se ha identificado un proyecto específico que se enfoque en un contexto de entidades crediticias. Esto indica que aún hay oportunidades para desarrollar soluciones innovadoras en este campo y adaptarlas a las necesidades específicas de este tipo de entidades en España y en Europa.

Capítulo 4. DEFINICIÓN DEL TRABAJO

4.1 JUSTIFICACIÓN

Uno de los principales retos a los que se enfrenta el sector bancario y ciertas instituciones financieras es el aumento del coste de los procesos de verificación KYC. Las entidades bancarias europeas dedican 5,7 millones de euros cada año a estos procesos (Ondato, 2022), con un gasto medio diario de casi 6.000 euros.

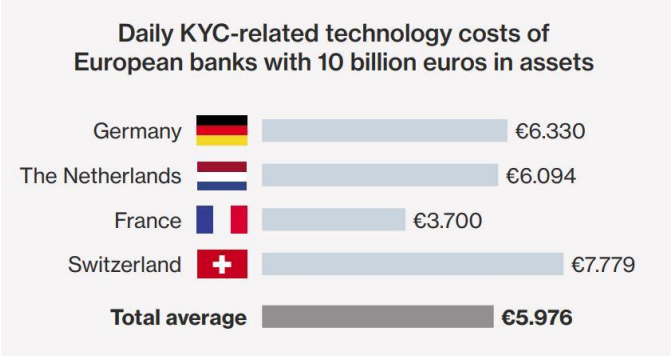


Ilustración 18: Gastos diarios en tecnología KYC de bancos europeos (Ondato, 2022)

Además de suponer un coste muy elevado para estas entidades, la lentitud de estos procesos también perjudica la experiencia de los clientes. Un estudio indica que, si la solicitud de un préstamo es un proceso de más de cinco minutos, la probabilidad de que el cliente abandone el proceso es del 60% o mayor. (Marous, 2021)

Una identidad financiera descentralizada disminuiría el coste de los procesos KYC y aumentaría su eficiencia, beneficiando a las entidades financieras y mejorando la experiencia de los clientes.

Además, esta identidad basada en *Blockchain* daría a los usuarios un mayor control sobre sus datos personales, ya que al descentralizar el proceso KYC no tendrían que proporcionar sus datos a cada institución con la que quieran solicitar créditos o préstamos.

También es destacable el crecimiento esperado del mercado de KYC electrónico. Según (Facts & Factors, 2023), la necesidad de procesos de verificación de identidad más eficientes y seguros y la creciente adopción de la tecnología *Blockchain*, la inteligencia artificial y el aprendizaje automático están impulsando aún más el mercado.

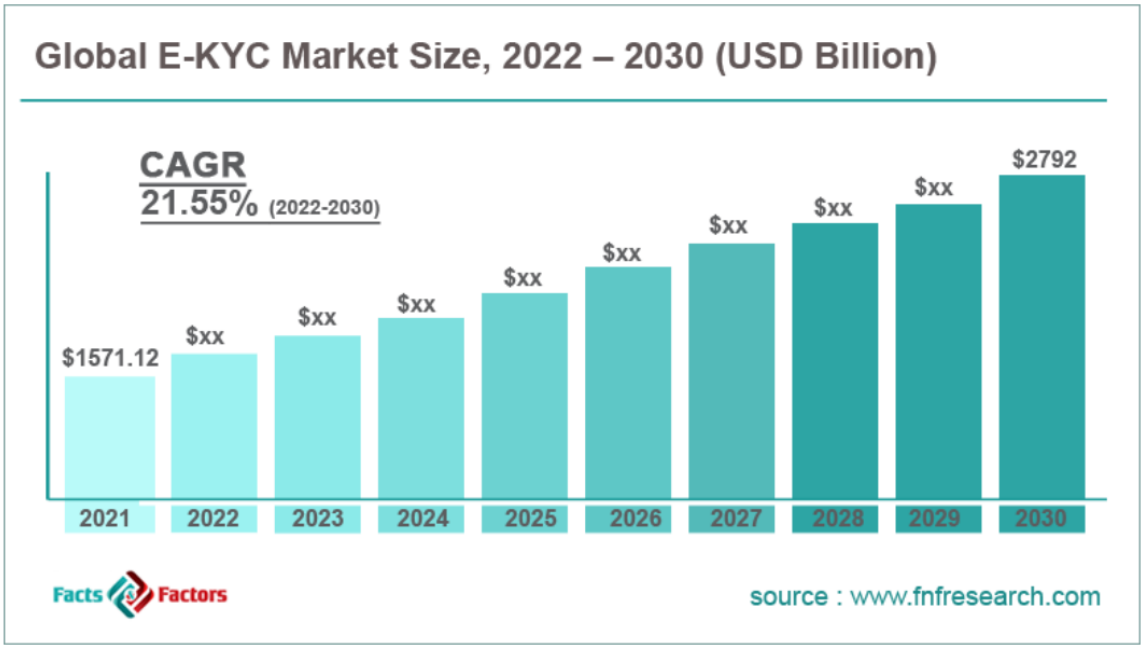


Ilustración 19: Tamaño global del mercado de e-KYC (Facts & Factors, 2023)

Por otro lado, en España no existe un *score* crediticio positivo. El CIRBE registra a todos los deudores en general, morosos y no morosos (Nacional Credit, 2023), y el fichero ASNEF registra a aquellos individuos que han incumplido alguna obligación dineraria (ASNEF, 2023). Muchas instituciones bancarias españolas utilizan su propio sistema de *scoring* bancario, basado en datos personales como el nivel de ingresos o la estabilidad del empleo del cliente, a la hora de valorar solicitudes de préstamos (BBVA). Esto forma parte del proceso KYC y les supone un elevado coste económico y temporal, ya que necesitan que los clientes aporten ciertos documentos que, en algunos casos, necesitan solicitar a terceros o a otras organizaciones.

4.2 OBJETIVOS

El objetivo principal de este proyecto es desarrollar una aplicación descentralizada basada en *Smart Contracts* para crear una identidad financiera digital personal y segura, en la cual los usuarios tengan el control completo sobre sus datos. Para obtener el resultado deseado se han de conseguir los siguientes objetivos:

i. **Agilización de procesos KYC.** Crear una aplicación que haga los procesos de identificación digital más eficientes, que esté disponible para cualquier persona y que proporcione a los usuarios una identidad digital segura, fiable y controlada por ellos mismos.
ii. **Identidad financiera o crediticia digital.** Proporcionar al usuario una identidad financiera digital respaldada por datos socioeconómicos y basada en *Blockchain* que le permita demostrar ciertos datos de su identidad (especialmente datos económicos para adquirir créditos) de manera irrefutable.
iii. **Aplicación web.** Crear un ejemplo de caso de uso en una aplicación web que muestre la solución propuesta por el proyecto.

4.3 METODOLOGÍA

Se sigue un modelo en cascada (*Waterfall*) para el desarrollo del proyecto.

En primer lugar, se lleva a cabo una investigación de las tecnologías a utilizar. Para ello se empieza con un estudio de la tecnología *Blockchain* y sus diferentes usos e integraciones con otras plataformas, y se hace uso de la documentación de las diferentes herramientas encontradas. Uno de los pasos iniciales es aprender a utilizar *Solidity*, el lenguaje de programación de *Smart Contracts*, de forma autodidacta. En esta etapa se hace también un análisis del estado del arte: se investiga sobre proyectos o sistemas existentes similares, sobre el estado de las identidades digitales, sobre las entidades crediticias, los burós de crédito negativos y positivos y los procesos KYC en las organizaciones, especialmente en España.

En la siguiente etapa se procede a la especificación y el diseño de la aplicación a desarrollar, con más enfoque a la parte de *backend*, al menos inicialmente. Para ello se emplean conocimientos previos de Java, Spring Boot, diseño web con HTML, CSS y JavaScript, y bases de datos SQL.

Durante la fase de desarrollo, se utilizan las tecnologías investigadas y se lleva a cabo un proceso de *testing* en paralelo para conseguir el resultado deseado. También de manera paralela, se va documentando el código y el proceso de desarrollo para facilitar la redacción de un análisis crítico de resultados al final del proyecto.

4.4 PLANIFICACIÓN Y ESTIMACIÓN ECONÓMICA

4.4.1 PLANIFICACIÓN TEMPORAL Y RESULTADOS

Dadas las limitaciones temporales y, por tanto, de alcance, del proyecto, se muestra en la siguiente imagen la planificación del desarrollo que se hizo al definir y comenzar el proyecto a desarrollar.

Actividad	Oct. 18-31	Nov. 1-30	Dic. 1-31	En. 1-31	Feb. 1-28	Mar. 1-31	Abr. 1-30	May. 1-31
Análisis								
Diseño								
Desarrollo								
Testing								
Documentación								

Ilustración 20: Planificación en modelo Waterfall

Como se muestra en el esquema anterior, es esencial que se documente el proyecto durante todas sus fases de diseño y desarrollo.

Se ha cumplido con las tareas marcadas tal y como aparecen en la imagen anterior. A continuación, se muestra la estimación temporal de las tareas indicadas.

Tarea	**Tiempo (horas)**
Definición del proyecto	10
Investigación y documentación de la tecnología *Blockchain*	23
Investigación sobre identidades digitales e identidades basadas en *Blockchain*	31
Investigación sobre procesos KYC y *scoring* crediticio en entidades bancarias	20
Aprendizaje de *Solidity*	17
Estudio de *Ganache* y *MetaMask*	10
Estudio de *JavaScript* y *Web3.js*	30
Estudio del entorno de desarrollo	10
Desarrollo del proyecto	100
Redacción de la memoria	50
Revisión de la memoria y posibles cambios	15
Elaboración de la presentación	12
Total	**328**

Tabla 1: Estimación temporal del proyecto

4.4.2 ESTIMACIÓN ECONÓMICA

Todo el *software* utilizado ha sido gratuito, por lo que para la estimación económica de los costes de elaboración del proyecto solo se ha tenido en cuenta el coste del personal.

Empleado	**Horas trabajadas**	**Coste por hora (€)**
Desarrollador	328	55
Jefe del proyecto	30	80
Total		**20.440€**

Tabla 2: Estimación económica de elaboración del proyecto

Además, para determinar si el proyecto es factible y fijar su presupuesto, se ha realizado un análisis de costes y beneficios en un escenario de cinco años de duración. En concreto, se han valorado tres escenarios posibles que se explicarán más adelante en este mismo capítulo.

4.4.2.1 Costes

Costes de desarrollo

Para el desarrollo "real" de la aplicación se usarán algunas plataformas gratuitas como *GitHub* y *Visual Studio Code*. El coste principal que engloba el desarrollo es el del personal.

Empleado	**Horas trabajadas**	**Coste por hora (€)**
Desarrollador #1	164	55
Desarrollador #2	164	55
Jefe del proyecto	30	80
Total		**20.440€**

Tabla 3: Coste de personal

Costes de configuración del nodo de Ethereum

Se ha estimado que la configuración de un nodo completo de *Ethereum* (*full node*) para la aplicación requerirá una inversión inicial de alrededor de 1200€.

Costes de mantenimiento

Para el mantenimiento del nodo de *Ethereum* y la aplicación web será necesario tener un sistema de almacenamiento, preferiblemente en la nube utilizando un servicio como AWS o similar.

También será necesario contar con personal en remoto que se encargue del mantenimiento del sistema a partir del segundo año, y también empleados en atención al cliente (preferiblemente a jornada parcial).

Elemento de mantenimiento	**Coste anual**
Almacenamiento en la nube	500€
Encargado del mantenimiento	30.000€
Atención al cliente	10.000€
Total	**40.500 €**

Tabla 4: Costes anuales de mantenimiento

Se ha considerado que el mantenimiento y la atención al cliente no entrarán a formar parte de los costes hasta el segundo año.

Costes de publicidad

Para los costes de publicidad se puede tener en cuenta un coste más elevado durante el primer año, y costes más bajos en los siguientes.

Se ha estimado un coste de 1.000€ el primer año, y 500€ los siguientes.

4.4.2.2 Ingresos

Los ingresos de la aplicación vendrían de cuotas mensuales pagadas por las organizaciones que participen. Se estima que durante el primer año participarán unas 40 organizaciones, principalmente organizaciones o entidades bancarias. La cuota mensual para estas organizaciones podría ser de unos 80€. En los siguientes años del proyecto, si se amplía a otro tipo de organizaciones, se podría llegar a contar con más de 300 organizaciones en el sistema.

4.4.2.3 Análisis de costes y beneficios

Se han realizado tres análisis de costes y beneficios a cinco años considerando tres escenarios o casos posibles: caso optimista, caso pesimista y caso realista.

En los siguientes escenarios y análisis no se ha incluido la inversión inicial de 21.640€, pero sí que se ha tenido en cuenta más adelante al calcular el ROI o Retorno Sobre la Inversión en el ROI.

La primera tabla muestra el análisis del caso optimista: la aplicación tiene mucho éxito, se integra fácilmente en el mercado y adquiere muchos usuarios y organizaciones que están interesadas en participar.

	Año 1	**Año 2**	**Año 3**	**Año 4**	**Año 5**
Ingresos (€)	38.400€	76.800€	115.200€	240.000€	336.000€
Costes (€)	41.500	41.000	41.000	41.000	41.000
Beneficios (€)	**-3.100**	**35.800**	**74.200**	**199.000**	**295.000**

Tabla 5: Análisis optimista de costes y beneficios

La segunda tabla muestra un análisis pesimista: el número de organizaciones que se unen al sistema crece muy lentamente o apenas crece de año a año, y además aumentan los costes tras una brecha de seguridad en el tercer año. Algunas organizaciones se dan de baja.

	Año 1	**Año 2**	**Año 3**	**Año 4**	**Año 5**
Ingresos (€)	33.600	43.200	48.000	43.200	42.240
Costes (€)	41.500	41.000	49.000	47.000	47.000
Beneficios (€)	**-7.900**	**2.200**	**-1.000**	**-3.800**	**-4.760**

Tabla 6: Análisis pesimista de costes y beneficios

Por último, la siguiente tabla muestra un análisis realista de los costes y beneficios a cinco años. El número de organizaciones partícipes crece a un ritmo más conservador, y los costes aumentan, pero no en gran cantidad.

	Año 1	**Año 2**	**Año 3**	**Año 4**	**Año 5**
Ingresos (€)	38.400€	52.800	54.720	63.360	81.600
Costes (€)	41.500	41.000	44.000	44.000	42.000
Beneficios (€)	**-3.100**	**11.800**	**10.720**	**19.360**	**39.600**

Tabla 7: Análisis realista de costes y beneficios

4.4.2.4 ROI

Se incluye un apartado dedicado al ROI (*Return On Investment*) o "retorno sobre la inversión" inicial del proyecto.

Aplicando a este caso una expresión básica del ROI:

$$ROI = \frac{(Beneficio\ total - Coste\ de\ inversión)}{Coste\ de\ inversión} \cdot 100$$

Tomando el beneficio total como la suma de los beneficios de los cinco años del caso realista, tenemos:

$$ROI = 262\%$$

El beneficio total sería 2,62 veces mayor que la inversión inicial.

Capítulo 5. FUNCIONALIDADES DEL SISTEMA

En este capítulo se abordan los detalles de la arquitectura, el diseño, las funcionalidades y el desarrollo del sistema que se han realizado para el proyecto.

La aplicación, que se llamado MyID, tiene dos tipos principales de usuarios: los usuarios (normales) y las organizaciones. Cada uno tiene funcionalidades diferentes.

No se han incluido como usuarios del sistema de MyID a las entidades o instituciones que "participan" en la aplicación, como el CIRBE, ASNEF, el Ministerio del Interior o la Agencia Tributaria o Hacienda. Esto se debe a que únicamente se han utilizado sus APIs, por lo que realmente no tienen una interacción directa con el sistema; es decir, no hacen uso del sistema, más bien MyID hace uso de sus servicios.

5.1 FUNCIONALIDAD DE USUARIO

Para empezar, cualquier persona puede registrarse como usuario de la plataforma; se trata de una plataforma pública. Para el registro, el usuario proporciona a la plataforma su nombre y apellidos, su DNI, su correo electrónico, un nombre de usuario para sus credenciales y una contraseña. Además, durante el registro se le pide al usuario que suba su DNI en un PDF oficial para poder verificarlo con la API del Ministerio del Interior. Si todos los datos son válidos y el PDF del DNI proporcionado concuerda con los datos de la API, se redirige al usuario al inicio de sesión para que pueda comenzar a usar la aplicación y a crear su identidad financiera.

Los usuarios crean su identidad financiera digital basada en un *rating* que les pueden otorgar ciertas organizaciones consideradas "legítimas" o "fiables". Por ejemplo, un banco o una entidad crediticia puede proporcionar puntos positivos a un usuario cuando devuelve un préstamo a tiempo, y también puede quitarle puntos si incumple el pago de alguna deuda. Nada más registrarse, se le otorga al usuario un *rating* inicial de 1. Su *rating* se irá

modificando según cómo sea su comportamiento financiero a medida que solicite préstamos o créditos. El funcionamiento de este *rating* financiero se explicará con más detalle al final de este capítulo.

Una vez iniciada la sesión correctamente, la aplicación proporciona a los usuarios diferentes funcionalidades. La principal es la funcionalidad para consultar su *rating* o puntuación de MyID, un valor que está asociado a su DNI en la *Blockchain* a través del *Smart Contract*. Esta funcionalidad requiere llamar a funciones del *Smart Contract* de la *Dapp* y ejecutar una función de visualización de la *Blockchain*.

Otra de las funcionalidades principales es que los usuarios también tienen la opción de subir su declaración de la renta para que este documento sea posteriormente verificado por las organizaciones del sistema usando una API de la Agencia Tributaria durante un eficiente proceso KYC.

En la aplicación web se han incluido también otras funcionalidades menores, como el acceso a información sobre el funcionamiento de MyID y sobre las entidades externas con las que colabora. Estas funcionalidades no son esenciales para el cumplimiento de los objetivos del proyecto, pero sí son un punto de partida para una aplicación o página web más accesible y amigable para los usuarios.

Cabe destacar que el usuario no tiene una dirección o *address* en la *Blockchain* de *Ethereum*. Esto se justifica principalmente por razones de accesibilidad. Para empezar, no todos los posibles usuarios de la aplicación conocen la tecnología *Blockchain*, por lo que supondría una barrera de entrada para ellos. Por otro lado, la creación de una dirección en *Ethereum* requiere el uso de recursos computaciones y la participación en el proceso de minería para asegurar la red. Esto implica una tarifa de transacción, o gasto de “gas”, que se debe pagar en la criptomoneda nativa de *Ethereum*, el *Ether* (ETH). Se ha supuesto que no todos los posibles usuarios de MyID tienen acceso a estas tecnologías, sea por motivos económicos o por otras razones.

5.1.1.1 Diagramas de casos de uso

Los diagramas de casos de uso son una herramienta utilizada en la metodología UML (Lenguaje de Modelado Unificado) para describir las interacciones entre un sistema y los actores o usuarios que interactúan con él. Estos diagramas ayudan a comprender cómo se utiliza un sistema desde la perspectiva del usuario, identificando los diferentes escenarios y acciones que pueden ocurrir.

Se han empleado este tipo de diagramas para definir de forma sencilla las funcionalidades del sistema desarrollado.

Caso de uso de usuarios autenticados

El siguiente diagrama muestra los casos de uso para usuarios que ya han iniciado sesión; es decir, los casos de uso para los usuarios ya autenticados en la aplicación.

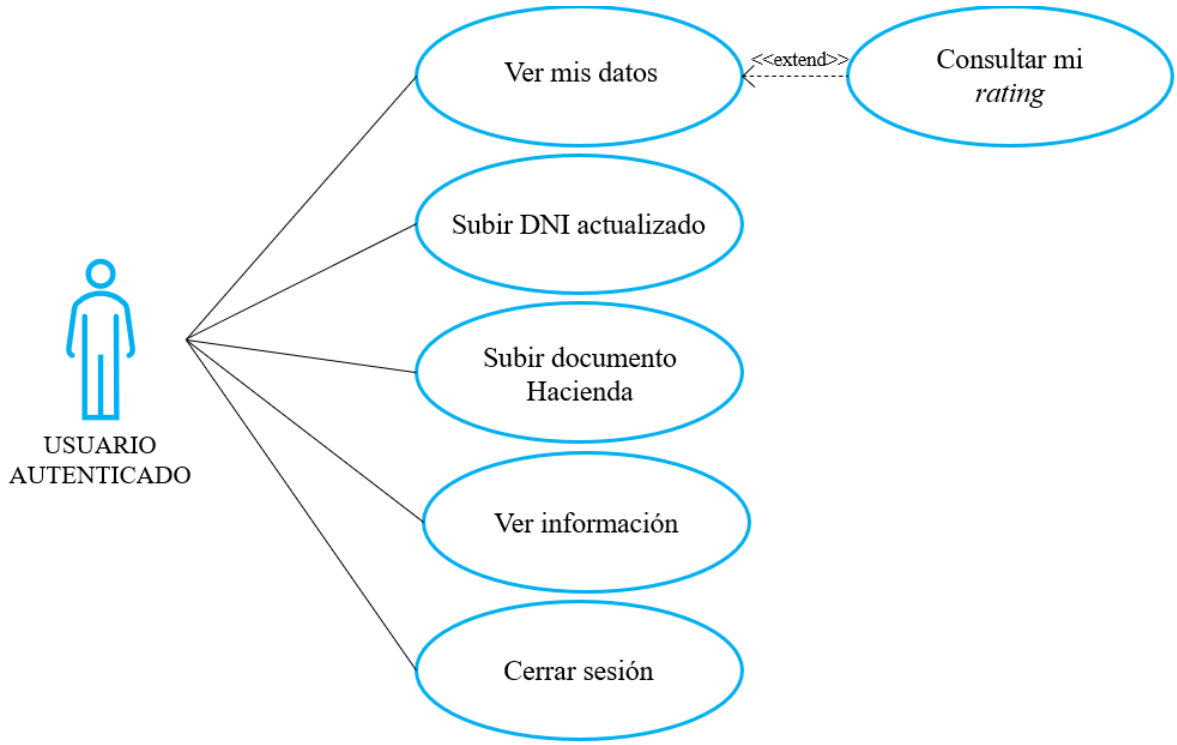


Ilustración 21: Diagrama de casos de uso para usuarios autenticados

Caso de uso de usuarios no autenticados

Este otro diagrama muestra los casos de uso para usuarios de la aplicación que no han iniciado sesión o que aún no están registrados.

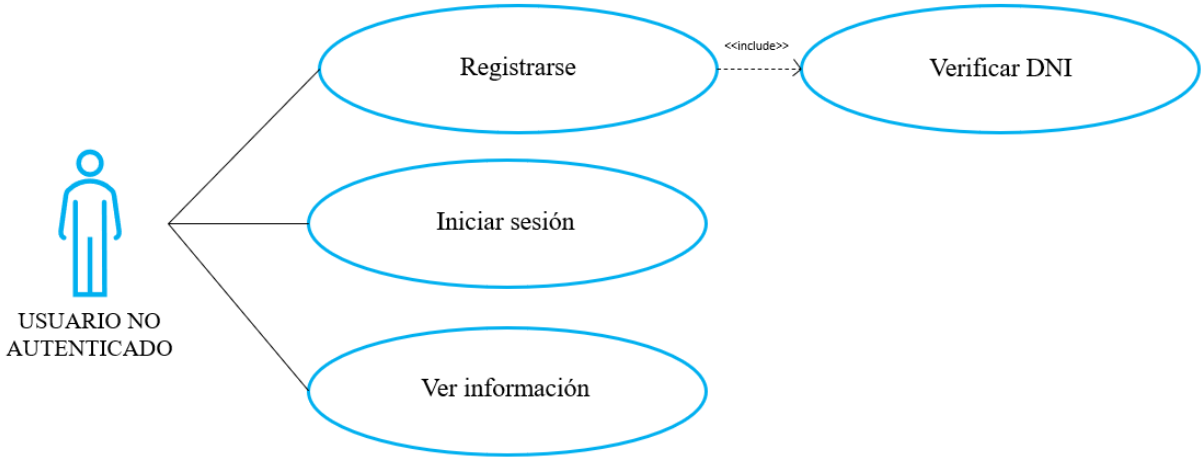


Ilustración 22: Diagrama de casos de uso para usuarios no autenticados

5.1.1.2 Diagrama de secuencia: verificación de DNI

Los diagramas de secuencia son una herramienta utilizada en UML (Lenguaje de Modelado Unificado) para visualizar y comprender la interacción entre objetos dentro de un sistema. Estos diagramas representan la secuencia de mensajes y acciones que ocurren entre los objetos a lo largo del tiempo, lo que permite analizar el flujo de eventos y la lógica del sistema.

Se han utilizado este tipo de diagramas para modelar y comunicar de manera clara y precisa el comportamiento dinámico del sistema, facilitando la identificación de colaboraciones entre objetos y el diseño de la lógica de procesamiento.

El siguiente diagrama de secuencia muestra la interacción de los diferentes elementos y componentes del sistema en el proceso de verificación del DNI cuando se registra un usuario.

Durante el proceso de registro, el usuario sube el PDF oficial de su DNI, y se genera el *hash* de dicho documento.

Se lleva a cabo un *GET Request* de la API del Ministerio del Interior que contiene un mapeo de DNI a *hash* del PDF oficial para todos los DNI del país cuyos dueños hayan autorizado estar incluidos en la API. Una vez obtenida la respuesta (*Response*) de la API, si se ha encontrado el DNI en la API, se compara el *hash* del documento que ha subido el usuario con el *hash* que su DNI tiene asociado en la API. Cabe destacar que los *hashes* de documentos se generan utilizando la función *SHA-256*, que genera un *hash* de 256 bits a partir de los datos de entrada.

En este diagrama se ha representado el caso en el que el DNI introducido y su documento son correctos y están registrados en la API del Ministerio del Interior. Una vez verificado el DNI y su *hash* con la API, se procede a guardar el DNI y su *hash* en *Blockchain* a través de los métodos del *Smart Contract*, como se muestra en el paso 1.4. Como se mencionado anteriormente, existe la posibilidad de modificar el DNI guardado en *Blockchain* en el caso de renovación del mismo. El diagrama de secuencia de esta otra funcionalidad es similar al mostrado a continuación.

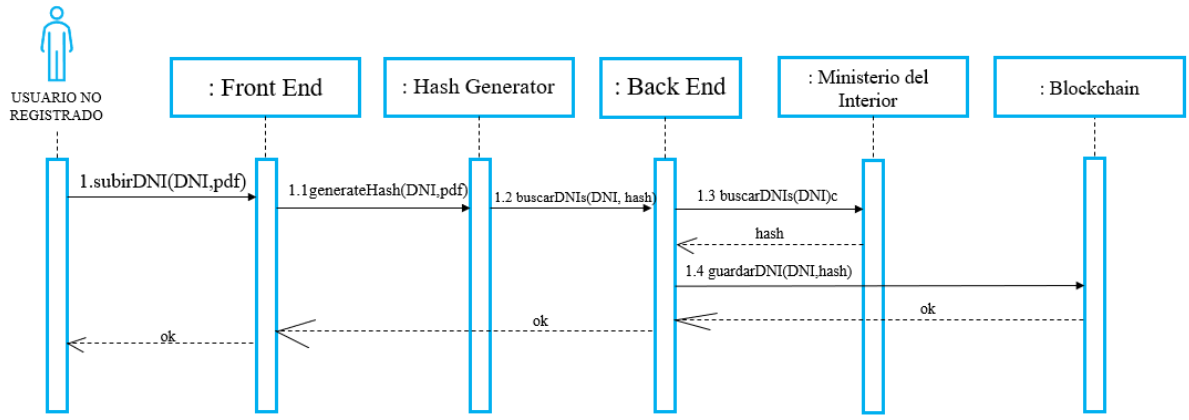


Ilustración 23: Diagrama de secuencia de verificación del DNI en el registro

En el diagrama anterior, el *Back End* representa la estructura de *Spring Boot* (*Service, Controller, Repository…*). Es evidente que el *Smart Contract* de *Blockchain* de *Ethereum*

también forma parte del *Back End* del sistema, pero hay un cierto nivel de aislamiento y separación entre estas dos partes.

5.2 FUNCIONALIDAD DE ORGANIZACIÓN

Se ha supuesto que las organizaciones interesadas en formar parte de MyID deben tener una cuenta en la red de *Ethereum*. Desde esta cuenta se llamarán a todas las funciones del *Smart Contract*, por lo que las operaciones realizadas por las organizaciones en la aplicación requerirán un gasto de ETH por parte de estas. Además, para el uso de la aplicación web necesitarán contar con una cartera o *Wallet* de *MetaMask* a la que el sistema pueda acceder fácilmente a través de la extensión de *MetaMask* que ofrecen muchos navegadores web. Esta *Wallet* debe estar conectada a la red de *Ethereum* correspondiente. Para este proyecto se ha creado una red de prueba usando *Ganache* en *localhost*.

Para registrarse en la plataforma, una organización debe proporcionar su nombre oficial, una contraseña y un código de verificación proporcionado por la Asociación Española de Banca (AEB). Además, la aplicación accederá a los datos de la cuenta configurada en la cartera de *MetaMask* a través de HTML para poder usar la dirección o *address* de la organización para las operaciones. Una vez recogidos el nombre de la organización y su dirección de *Ethereum*, MyID hará uso de una API externa de la AEB para verificar que forma parte de una asociación de entidades financieras legítimas.

Si todo es correcto, una vez registradas, se redirige a las organizaciones a la página de inicio. Para la autenticación durante el inicio de sesión, y para todo el uso de la aplicación, es necesario tener conectada la *Wallet* a la red de *Ethereum*.

Las organizaciones también tienen un *rating*, que inicialmente tiene un valor de 1, al igual que para los usuarios. Una vez iniciada la sesión, las organizaciones tienen acceso a muchas funcionalidades. Cabe destacar que algunas de estas funcionalidades serán accesibles o no según este *rating*.

Las organizaciones pueden ver el *rating* de los usuarios y otorgarles puntos. Por ejemplo, si un usuario devuelve un préstamo a tiempo a un banco, el banco puede darle puntos positivos por ello. En caso contrario, la organización puede quitar puntos al usuario. Así contribuyen a la creación de las identidades financieras de los usuarios, y a la mejora de la fiabilidad y del sistema.

Las organizaciones también pueden puntuar a otras organizaciones, y pueden visualizar su propio *rating*. Al puntuar a otras organizaciones, contribuyen a la creación de una plataforma fiable y segura.

Otra funcionalidad que tienen las organizaciones es que pueden verificar si los documentos de la declaración de la renta proporcionados por sus clientes son válidos o están actualizados. Tienen la opción de subir un documento y obtener su verificación inmediatamente a través de una API de la Agencia Tributaria o Hacienda. También pueden verificar el DNI de un cliente, utilizando la misma API que utilizan los usuarios cuando se registran en la plataforma.

Además, pueden comprobar si un cliente está incluido en el fichero ASNEF a través de otra API externa de ASNEF o si tiene algún préstamo buscando su DNI a través de una API del CIRBE.

En este apartado se ha incluido el diagrama de casos de uso para organizaciones autenticadas y no autenticadas, y algunos diagramas de secuencia que representan algunas de las funcionalidades esenciales mencionadas anteriormente. En concreto, se han incluido diagramas de secuencia para la puntuación de usuarios (positiva y negativa) y para la búsqueda de usuarios en la API del CIRBE. La búsqueda de usuarios en la API de ASNEF es similar a la del CIRBE, y la verificación de legitimidad de la API de la AEB sigue un proceso prácticamente idéntico a la verificación del DNI de usuario mostrada en la sección de funcionalidades previa. Por estas razones no se han incluido diagramas de secuencia de estos últimos casos de uso mencionados.

5.2.1.1 Diagramas de casos de uso

Caso de uso de organizaciones autenticadas

El siguiente diagrama muestra los casos de uso para una organización registrada.

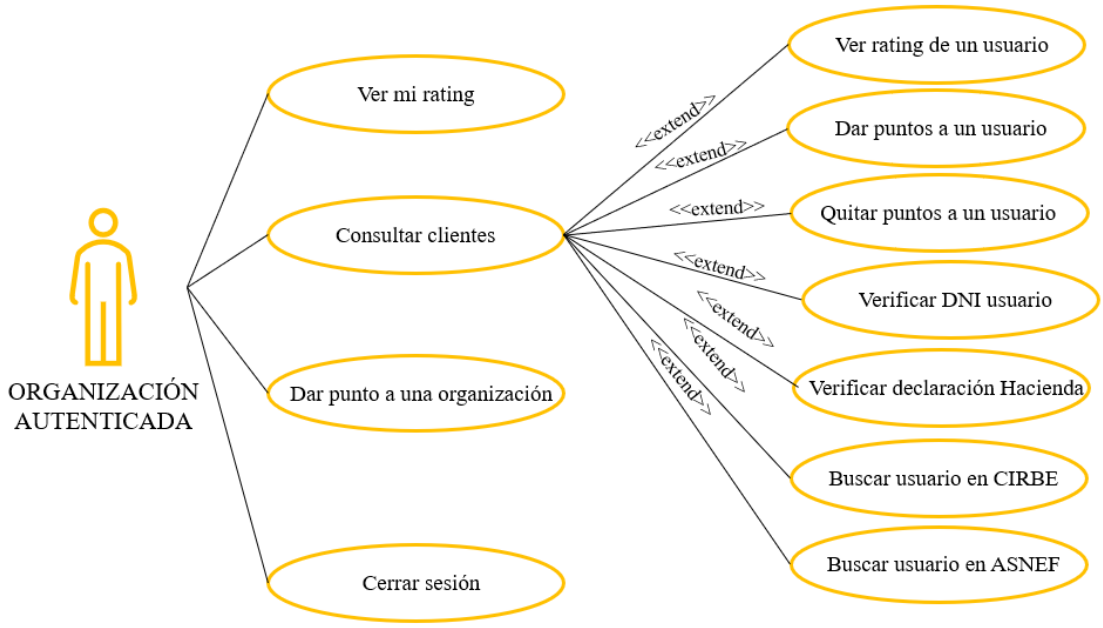


Ilustración 24: Diagrama de casos de uso para organizaciones registradas

Caso de uso de organizaciones no autenticadas/no registradas

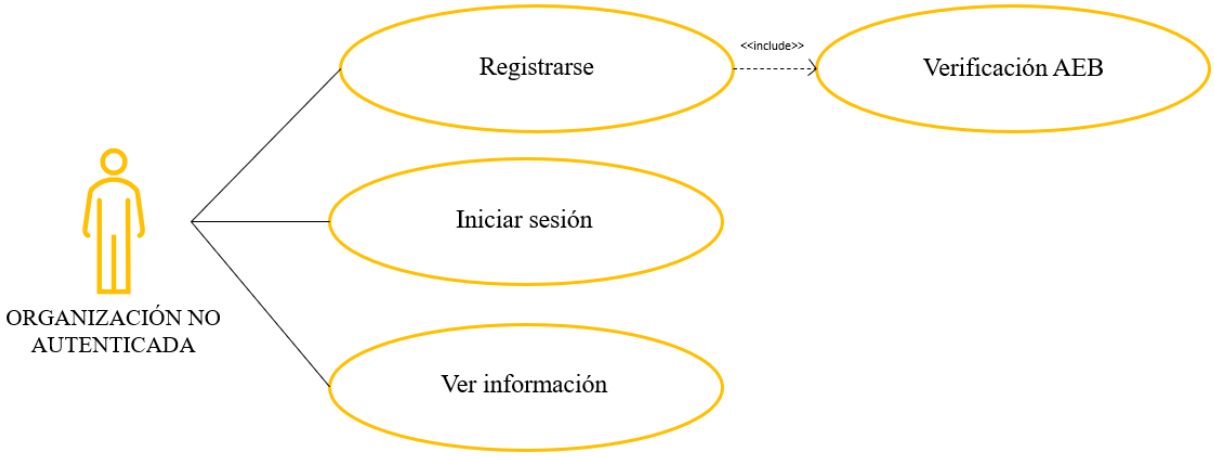


Ilustración 25: Diagrama de casos de uso para organizaciones no autenticadas

5.2.1.2 Diagramas de secuencia

Diagrama de secuencia de puntuación de un usuario

El siguiente diagrama de secuencia muestra las interacciones entre los diferentes elementos del sistema en el caso de uso de puntuar a un usuario. Se ha incluido únicamente el caso de la puntuación positiva, pero el caso de la puntuación negativa o retiro de puntos es prácticamente igual.

La puntuación o *rating* de los usuarios no se guarda en la base de datos de SQL conectada a la estructura de *Spring Boot*, sino que queda guardada únicamente en *Blockchain*. Por tanto, el diagrama de secuencia para este caso de uso no incluye el *Back End* que se ha mencionado previamente; solo incluye la parte del *Smart Contract* como se muestra a continuación.

También cabe destacar que antes de llevar a cabo el cambio de la puntuación, se comprueba la puntuación de la propia organización, ya que según su *rating* podrá añadir o quitar más o menos puntos a los usuarios. La puntuación entre organizaciones es similar, pero no se puntúa más o menos según el propio *rating*.

El "resultado" devuelto por el *Smart Contract* depende de si el DNI que la organización quiera puntuar está o no registrado en el mapeo de puntuaciones del *Smart Contract*. Se notificará a la organización si el usuario dueño del DNI no está registrado.

Además, la función de puntuación de usuarios en el *Smart Contract* es diferente según la puntuación de la organización. Esto se explicará de forma más detallada al final de este capítulo.

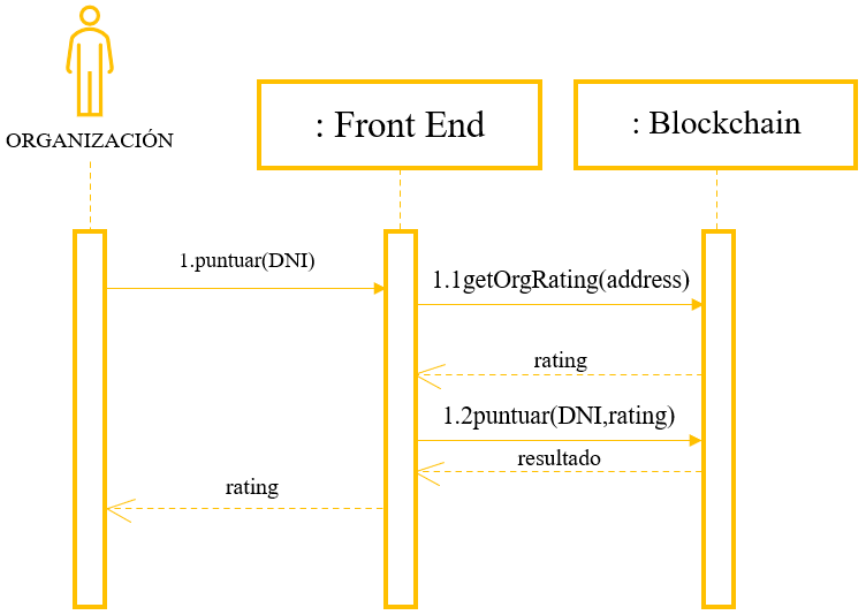


Ilustración 26: Diagrama de secuencia para la puntuación de usuarios

Diagrama de secuencia de búsqueda de un usuario en el CIRBE

El siguiente diagrama de secuencia muestra las interacciones entre los diferentes elementos del sistema en el caso de uso de buscar a un usuario en el CIRBE. Se ha incluido únicamente este caso de búsqueda porque para ASNEF el igual.

La búsqueda en la API del CIRBE (y en el resto de APIs) solo es accesible para organizaciones con una cierta puntuación, por lo que esta funcionalidad hace uso de las dos "partes" del *Back End* que se han mencionado anteriormente.

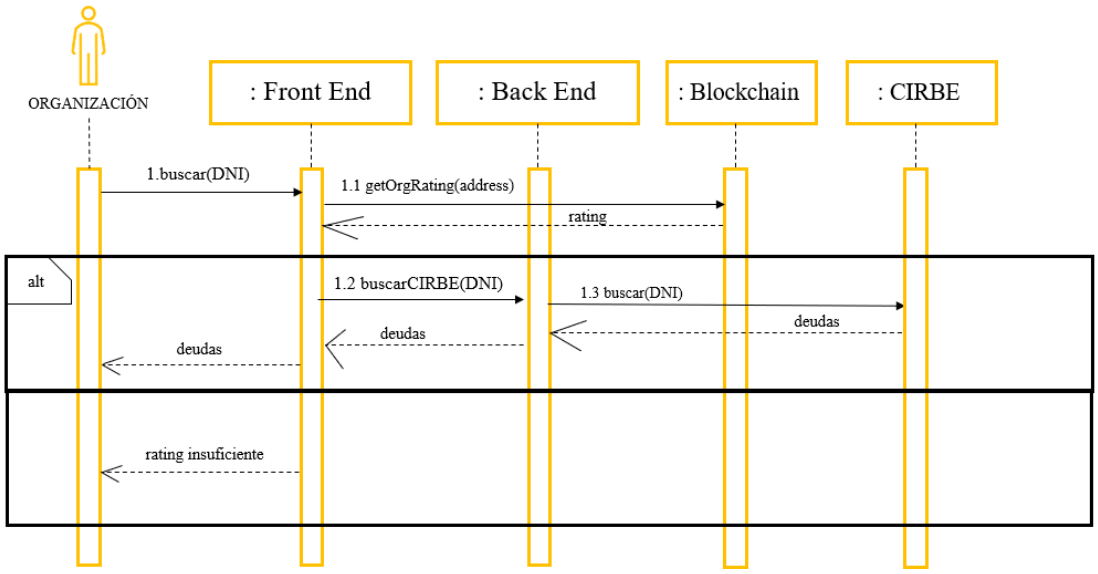


Ilustración 27: Diagrama de secuencia para la puntuación de usuarios

5.3 NAVEGABILIDAD EN LA DAPP

El siguiente diagrama de navegabilidad engloba casi todas las funcionalidades que proporciona la aplicación, para aportar más claridad sobre el funcionamiento del sistema que se ha desarrollado.

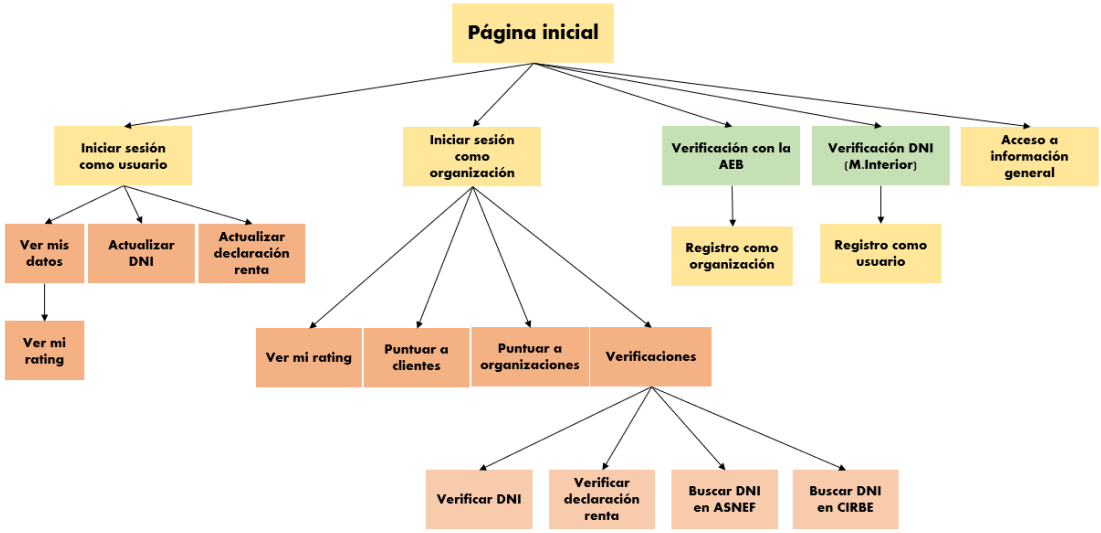


Ilustración 28: Navegabilidad en la Dapp

Desde la página inicial, se puede acceder a diferentes secciones a través de una barra de navegación: *Personal*, *Empresa*, *Sobre MyID*, *Acceso* y *Registro*.

En la pestaña *Personal*, aparecen varias secciones informativas sobre la posibilidad de crear una cuenta de usuario en la aplicación.

En la pestaña *Empresa*, también aparecen varias secciones informativas sobre la creación de una cuenta de empresa u organización.

En *Sobre MyID*, se puede acceder a una información más completa y detallada sobre la aplicación.

En *Acceso* se permite iniciar sesión a usuarios y a organizaciones.

En *Registro*, tanto usuarios como organizaciones pueden crear cuentas en la aplicación. Para ello se llevan a cabo las verificaciones explicadas en el apartado anterior haciendo uso de APIs externas.

Una vez iniciada la sesión como usuario, se puede acceder a las funcionalidades mencionadas en diferentes pantallas o secciones de la web: *Ver mis datos* (y *Ver mi rating*), *Actualizar DNI* y *Actualizar declaración de la renta*.

Para las organizaciones que han iniciado sesión ocurre de forma similar. Las diferentes pantallas a las que se puede acceder son: *Ver mi rating*, *Colaboración* (para ver las APIs externas con las que trabaja la aplicación y consultar sus datos), *Rating de clientes* y *Rating de organizaciones*.

No se ha incluido en el diagrama de navegabilidad para simplificar el esquema, pero la barra de navegación para usuarios y organizaciones autenticados incluye también una opción para cerrar sesión.

5.4 FUNCIONAMIENTO DEL SISTEMA DE RATING O PUNTUACIÓN

El sistema de *rating* o puntuación de usuarios y organizaciones es similar a los sistemas de *scoring* financiero que utilizan algunas entidades bancarias españolas.

Tanto para usuarios como organizaciones, el *rating* inicial cuando se dan de alta en la plataforma tiene un valor de 1. Las entidades que tienen un *rating* igual o superior a un umbral de 6 son consideradas "fiables" o "legítimas". Las organizaciones legítimas pueden aumentar o disminuir el *rating* de los usuarios en dos o cuatro unidades. Esto se ha implementado de esta forma para que las entidades bancarias, por ejemplo, otorguen más puntos a usuarios que pagan un préstamo hipotecario que a usuarios que pagan préstamos de menor envergadura.

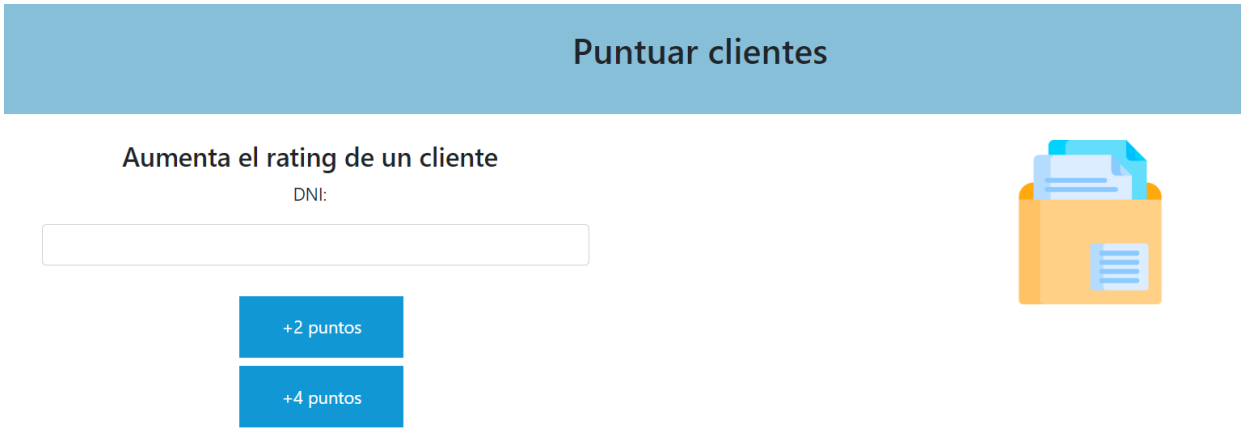


Ilustración 29: Puntuación de clientes para organizaciones legítimas

Todas las organizaciones pueden aumentar la puntuación de otras organizaciones en saltos de una unidad. Las organizaciones con un *rating* inferior a 6 pero superior o igual a 1 pueden aumentar el *rating* de los usuarios en una unidad.

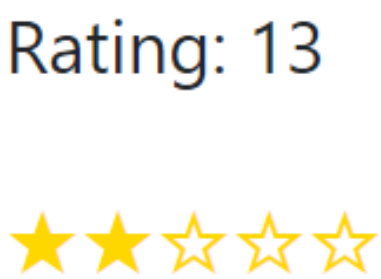


Ilustración 30: Ejemplo de visualización del rating para usuarios y organizaciones

Las organizaciones con un *rating* igual o superior a 8 pueden acceder a la información de las APIs del Ministerio del Interior, la Agencia Tributaria o Hacienda, ASNEF y CIRBE. La información que una organización obtiene de esta API no influye directamente en la puntuación del usuario que queda guardada en la *Blockchain*, ya que estas entidades no participan en el sistema de forma directa. Sin embargo, pueden influir indirectamente en el *rating*, ya que las organizaciones podrían elegir puntuar positiva o negativamente a un usuario a partir de la información de estas APIs.

Las organizaciones no pueden votarse a sí mismas.

El *rating* mínimo tanto para usuarios y organizaciones es 1.

Como se muestra en la Ilustración 30: Ejemplo de visualización del rating para usuarios y organizaciones, el *rating* se visualiza de forma numérica y de forma gráfica, con cinco estrellas a rellenar. Aunque las estrellas hacen el *rating* más visual y amigable para usuarios y organizaciones, el *rating* numérico es realmente el que mayor información aporta, porque indica más claramente:

- Cuántas organizaciones han “verificado” a la organización. Las organizaciones votan en saltos de una unidad, por lo que el *rating* numérico de una de ellas indica cuántas otras la consideran legítima o verificada. Se ha considerado que estar verificada por 32 organizaciones o más supone un *rating* de 5 estrellas para la organización.

- Qué tipos de comportamientos financieros positivos ha tenido el usuario. Como se explicó previamente, las organizaciones darán más puntos a los usuarios por sus comportamientos positivos respecto a productos financieros de altos intereses, como hipotecas. Se ha considerado que tener un *rating* numérico de 32 implica tener 5 estrellas para el usuario. Tener un *rating* de 32 implica haber devuelto correctamente o bien dieciséis préstamos de menor envergadura, o bien ocho préstamos de gran envergadura, o bien una combinación de ambos (que sería lo más habitual para el cliente medio).

Se incluyen ambos tipos de visualización para mejorar la parte *Front* de la aplicación web.

Capítulo 6. ARQUITECTURA DEL SISTEMA

Para poder implementar las funcionalidades descritas en el capítulo anterior, ha sido necesario integrar diferentes soluciones de software. La siguiente figura muestra la arquitectura de la *Dapp* que se ha desarrollado para cumplir con los requerimientos del proyecto, utilizando las tecnologías descritas en el Capítulo 2.

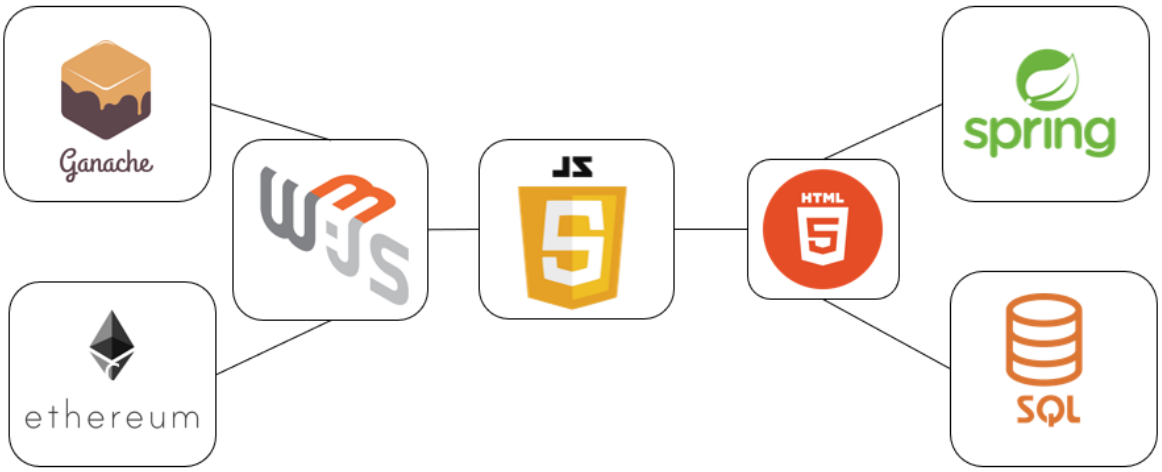


Ilustración 31: Arquitectura del sistema

El *Front End* de la aplicación se ha desarrollado con HTML y CSS.

Es sencillo ver que la arquitectura propuesta para la *Dapp* tiene dos "partes" de *Back End*. Por un lado, está la parte del *Smart Contract*, y por otro lado la parte de *Back End* que tienen usualmente las aplicaciones web que se desarrollan usando *Java* y *Spring Boot*.

Como se explicó anteriormente, el *Smart Contract* de la *Dapp* se ha programado en lenguaje *Solidity* y utilizando *Visual Studio Code* como editor. Una vez programado el *Smart Contract*, para desplegarlo y testearlo se necesita un nodo de *Ethereum* simulado en *Ganache*. Esta parte del *Back End* se comunica con el *Front* a través de la librería *Web3.js* integrada en *JavaScript*.

La otra parte del Back End se ha programado en lenguaje Java utilizando la herramienta *Spring Boot*. La herramienta *Spring Boot* ha servido también para trabajar con almacenamiento de datos en bases de datos estructuradas compatibles con SQL. Esta otra parte del *Back End* también se comunica con el *Front* utilizando *JavaScript*.

La estructura de paquetes del proyecto se puede visualizar a continuación, en la Ilustración 32: Estructura del proyecto - Visual Studio Code:

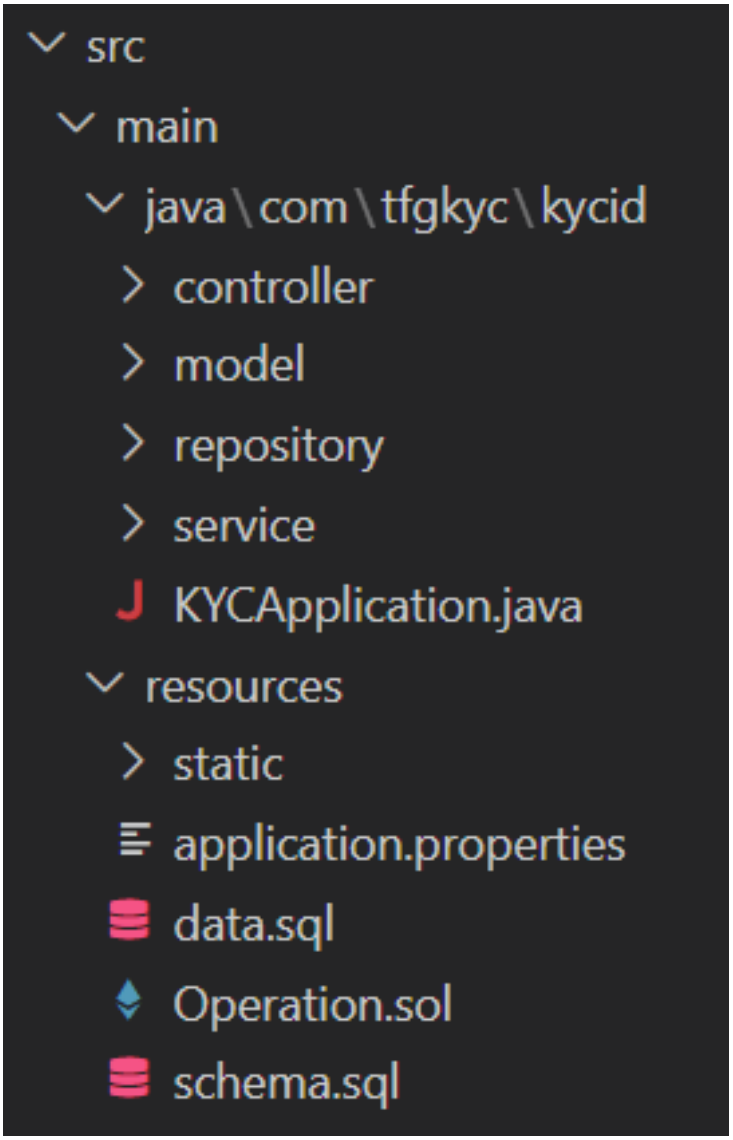


Ilustración 32: Estructura del proyecto - Visual Studio Code

La ruta *java/com/tfgkyc/kycid* incluye la estructura básica de un proyecto de *Spring Boot*, que se explicará más en detalle en el siguiente capítulo. Esta sección incluye las siguientes subcarpetas:

- Controller
- Service
    - DTO
    - Service Implementer
- Repository
- Table

La carpeta de recursos o *resources* está formada principalmente por los recursos estáticos del sistema, que en este caso componen la parte frontal de la aplicación: las páginas HTML, sus hojas de estilos en CSS, sus ficheros de código *JavaScript* y sus imágenes o iconos.

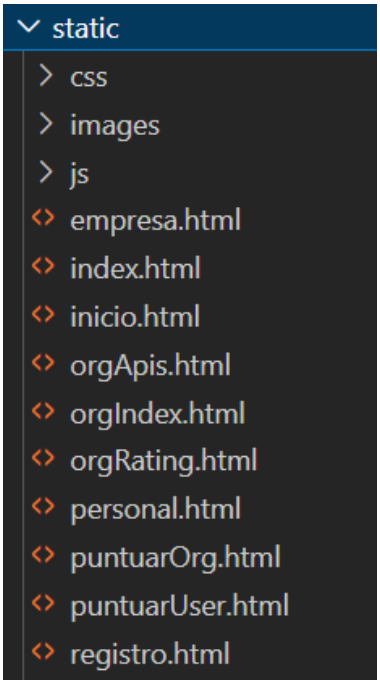


Ilustración 33: Elementos estáticos

El archivo *application.properties* es un archivo de configuración que se utiliza para establecer propiedades y configuraciones específicas de la aplicación. En este archivo, se han establecido propiedades como la configuración de la base de datos, la configuración del servidor y las rutas de recursos.

Este archivo está relacionado, por tanto, con los ficheros *schema.sql* y *data.sql* que componen la base de datos de la aplicación.

- En *schema.sql* se crean las tablas de la base de datos.
- En *data.sql* se inicializan dichas tablas si es necesario.

Por último, el fichero *Operation.sol* es el *Smart Contract* de la aplicación, escrito en *Solidity*. Su funcionamiento se explicará en más detalle en el siguiente capítulo.

Capítulo 7. DESARROLLO DE LA DAPP

7.1.1 SMART CONTRACT

El *Smart Contract* de la *Dapp* está escrito en *Solidity*.

Se han usado *mappings* para almacenar:

- El DNI de cada usuario mapeado a su *rating*
- La dirección de *Ethereum* de cada organización mapeada a su *rating*
- La dirección de *Ethereum* de cada organización mapeada al nombre de la organización
- El nombre de un fichero (DNI o declaración de la renta) asociado a su *hash* para las verificaciones de documentos

```
contract Operation {

  // Ratings de usuario
  mapping(string => uint) userRatings;

  // Ratings de organizaciones
  mapping(address => uint) orgRatings;

  // Nombres de organizaciones
  mapping(address => string) orgNames;

  // Nombres de organizaciones (invertido)
  mapping(string => address) orgAddresses;

  // Ficheros
  mapping(string => bytes32) private fileHashes;
```

Fragmento de código 1: Mappings del Smart Contract

También se ha utilizado otro *mapping* para almacenar el nombre de cada organización mapeada a su dirección de *Ethereum*. Los *mappings* en *Solidity* no son iterables, y tener las dos versiones facilita muchas operaciones.

Las funciones del *Smart Contract* permiten a los otros elementos del sistema interactuar con él. En *Solidity*, las funciones pueden ser de varios tipos (Solidity, 2016):

- ***Public***. Cualquier persona con una cuenta de *Ethereum* puede llamar a este tipo de función. La mayoría de las funciones implementadas son de este tipo.
- ***Internal***. Una función de este tipo solo puede ser llamada desde el interior del *Smart Contract*.
- ***Payable***. Una función *payable* puede recibir *Ethers*.
- ***View***. Este modificador indica que la función accede y visualiza datos del *Smart Contract*, pero no modifica *Blockchain*.
- ***Pure***. Este modificador es similar a *view*, pero ni modifica ni accede a datos del contrato.

Las siguientes funciones se encargan de actualizar la puntuación de un usuario cuando una organización le otorga o quita puntos. Son funciones que solo las organizaciones pueden acceder.

```
  // DAR 1 o 2 PUNTOS A UN USUARIO
  function updateUserRating(string memory dni, uint puntuacion) public returns
(bool,uint){
    if (orgRatings[msg.sender] >= 6 && userRatings[dni] != 0){
      userRatings[dni] = userRatings[dni] + puntuacion;
      return (true,userRatings[dni]);
    }else if (orgRatings[msg.sender] >= 1 && orgRatings[msg.sender] <= 5 &&
userRatings[dni] != 0){
      userRatings[dni] = userRatings[dni] + 1;
      return (true,userRatings[dni]);
    }else{
      return (false,0);
    }
  }

  // QUITAR 1 o 2 PUNTOS A UN USUARIO
  function removeUserVote(string memory dni, uint puntuacion) public returns
(bool,uint){
    if (orgRatings[msg.sender] >= 6 && userRatings[dni] != 0){
      if (userRatings[dni] <= puntuacion){
        userRatings[dni] = 1;
        return (true,userRatings[dni]);
      }else{
        userRatings[dni] = userRatings[dni] - puntuacion;
        return (true,userRatings[dni]);
      }
    }else if (orgRatings[msg.sender] >= 1 && orgRatings[msg.sender] <= 5 &&
userRatings[dni] != 0){
      if (userRatings[dni] > 1){
```

```
      userRatings[dni] = userRatings[dni] - 1;
      return (true,userRatings[dni]);
    }else{
      return (true,userRatings[dni]);
    }
  }else{
    return (false,0);
  }
}
```

Fragmento de código 2: Funciones de puntuación de clientes o usuarios

Una vez llamadas estas funciones, hacen la verificación del *rating* de las organizaciones que las han llamado para:

- Puntuar al usuario con la puntuación elegida por la organización
- Puntuar al usuario en cantidades de una unidad
- No puntuar al usuario si la organización no tiene suficiente *rating* asociado a su dirección de *Ethereum*

También comprueban que el DNI del usuario al que se está intentando "votar" está incluido en el *mapping* de *ratings* de usuarios.

Las organizaciones también pueden puntuar a otras organizaciones accediendo a la siguiente función del *Smart Contract*.

```
// AUMENTAR EL RATING DE UNA ORG
function updateOrgRating(address orgAddress) public returns (bool, uint){
  if (orgRatings[orgAddress] != 0){
    orgRatings[orgAddress] = orgRatings[orgAddress] + 1;
    return (true,orgRatings[orgAddress]);
  }else{
    return (false,0);
  }
}
```

Fragmento de código 3: Función de puntuación de organizaciones

Las organizaciones y usuarios pueden acceder a su propio *rating*:

```
// BUSCAR USER RATING
function getUserRating(string memory dni) public view returns (uint){
```

```
  return userRatings[dni];
}

// BUSCAR ORG RATING
function getOrgRating(string memory orgname) public view returns (uint){
  return orgRatings[orgname];
}
```

Fragmento de código 4: Funciones de búsqueda de puntuaciones

El *Smart Contract* también incluye una función que devuelve el nombre de la organización a partir de la dirección:

```
// BUSCAR ORG NAME
function getOrgName(address orgAddress) public view returns (string memory){
  return orgNames[orgAddress];
}
```

Fragmento de código 5: Función de búsqueda de nombre de organización

La función para añadir usuarios al sistema puede ser accedida por cualquier usuario que se registre en la web de la plataforma.

```
// AÑADIR USUARIO
function addUser(string memory dni) public returns (uint) {
  userRatings[dni] = 1; // por defecto
  return (userRatings[dni]);
}
```

Fragmento de código 6: Función para registrar nuevos usuarios en la red

Las funciones para registrar organizaciones son llamadas por ellas mismas a la hora de registrarse en la plataforma.

```
// AÑADIR ORG
function addOrg(address newAddress, string memory orgname) public{
  orgRatings[newAddress] = 1; // por defecto
  orgNames[newAddress] = orgname;
  orgAddresses[orgname] = newAddress;
}
```

Fragmento de código 7: Función para registrar nuevas organizaciones en la red

Para la subida del *hash* de documentos, y también para la comparación de *hashes* del *Smart Contract* y de la base de datos de SQL que se hace en *JavaScript*, se utilizan las siguientes funciones.

```
  // Emitir evento cuando se suba un PDF
  event FileUploaded(string indexed fileName, bytes32 hash);

  // SUBIR UN PDF
  function uploadPDF(string memory fileName, bytes memory hash) public{
    bytes32 hashBytes32 = bytesToBytes32(hash);
    fileHashes[fileName] = hashBytes32;
    emit FileUploaded(fileName,hashBytes32);
  }

  // FUNCION PARA CONVERTIR DE BYTES A BYTES32
  function bytesToBytes32(bytes memory data) internal pure returns (bytes32
result) {
    require(data.length == 32, "Invalid input length");
    assembly {
        result := mload(add(data, 32))
    }
  }

  // OBTENER EL HASH DE UN FICHERO SUBIDO PREVIAMENTE
  function getHashByFileName(string memory fileName) public view returns
(bytes32) {
    return fileHashes[fileName];
  }
```

Fragmento de código 8: Funciones para el tratado del hash de documentos

Por último, el siguiente fragmento debe ser la primera línea del *Smart Contract* programado en *Solidity*.

```
pragma solidity >=0.7.0 <0.9.0;
```

Fragmento de código 9: Directiva pragma Solidity

La declaración anterior es una directiva que especifica la versión de *Solidity* que se debe usar para compilar el *Smart Contract*.

En este caso, se indica que se debe utilizar una versión de Solidity igual o superior a 0.7.0 y menor a 0.9.0. Esto significa que el *Smart Contract* se escribirá y compilará utilizando las características y sintaxis disponibles en esa versión específica de *Solidity*.

El uso de una directiva pragma es importante porque garantiza la compatibilidad y la consistencia en el desarrollo de *Smart Contracts*. Diferentes versiones de *Solidity* pueden

introducir cambios en la sintaxis o comportamiento del lenguaje, por lo que especificar una versión particular ayuda a evitar problemas de compatibilidad y asegura que el contrato se compile y se ejecute correctamente.

Además, el uso de una directiva pragma también puede tener implicaciones en la seguridad y la estabilidad del contrato inteligente. Versiones más recientes de Solidity pueden incluir mejoras de seguridad y correcciones de errores, por lo que es importante utilizar una versión actualizada para aprovechar estas mejoras.

El *Smart Contract* contiene otras funciones auxiliares que no se han incluido en esta sección.

7.1.2 GANACHE

Como se explicó en el Capítulo 2, se ha utilizado la aplicación de escritorio *Ganache* para crear diferentes cuentas para las organizaciones, indicar sus saldos iniciales, tener acceso a sus direcciones en la red y para ver las transacciones realizadas por cada una. Esto ha permitido trabajar con las cuentas de forma sencilla y visual.

Para este proyecto, se ha simulado un nodo de *Ethereum* con 100 posibles cuentas o direcciones.

Las cuentas están asociadas en el *Smart Contract* a los nombres de las organizaciones, además de a sus *ratings*.

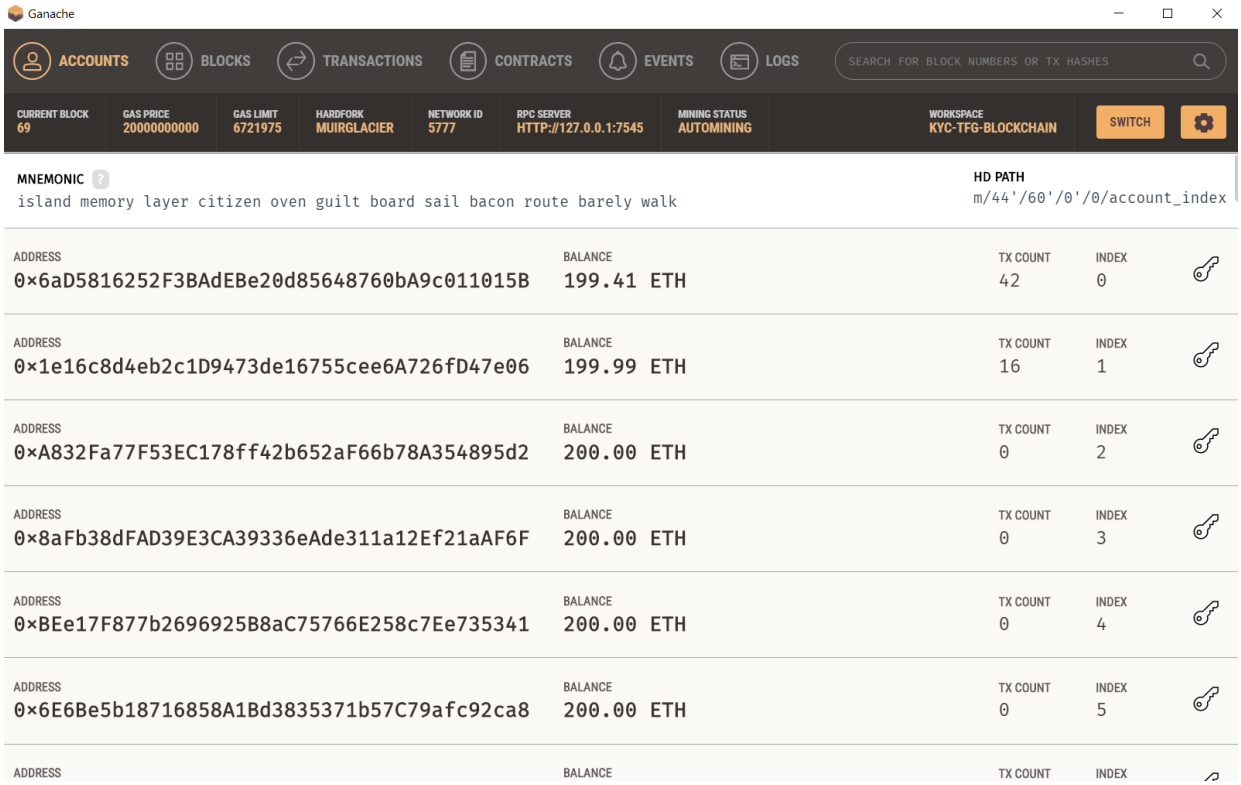


Ilustración 34: Cuentas y direcciones en Ganache

7.1.3 METAMASK

Como se explicó en el Descripción de las Tecnologías, se ha integrado la cartera o *wallet* de *MetaMask* en la aplicación desarrollada a través de la extensión del navegador. Para el desarrollo del proyecto se ha utilizado el navegador de *Chrome*.

La cartera de *MetaMask* se conecta a la red local, que es en la que está desplegada la red de pruebas de *Ethereum* creada en *Ganache*. Así, desde la extensión, que se puede abrir en la parte superior derecha del navegador como se muestra en la Ilustración 35: Ejemplo de uso de la extensión de MetaMask, se puede acceder a todas las cuentas desplegadas (con la dirección y la clave privada que proporciona la red de *Ganache*) y hacer operaciones desde ellas.

Cabe destacar que para poder tener acceso a todas estas cuentas a través de la extensión es necesario, en primer lugar, conectar la cartera a la red de *Ganache* y, en segundo lugar,

importar las cuentas. Para importar las cuentas se debe introducir tanto la dirección o *address* de estas como su clave privada o *private key*, que se trata de una clave compuesta por 64 caracteres hexadecimales.

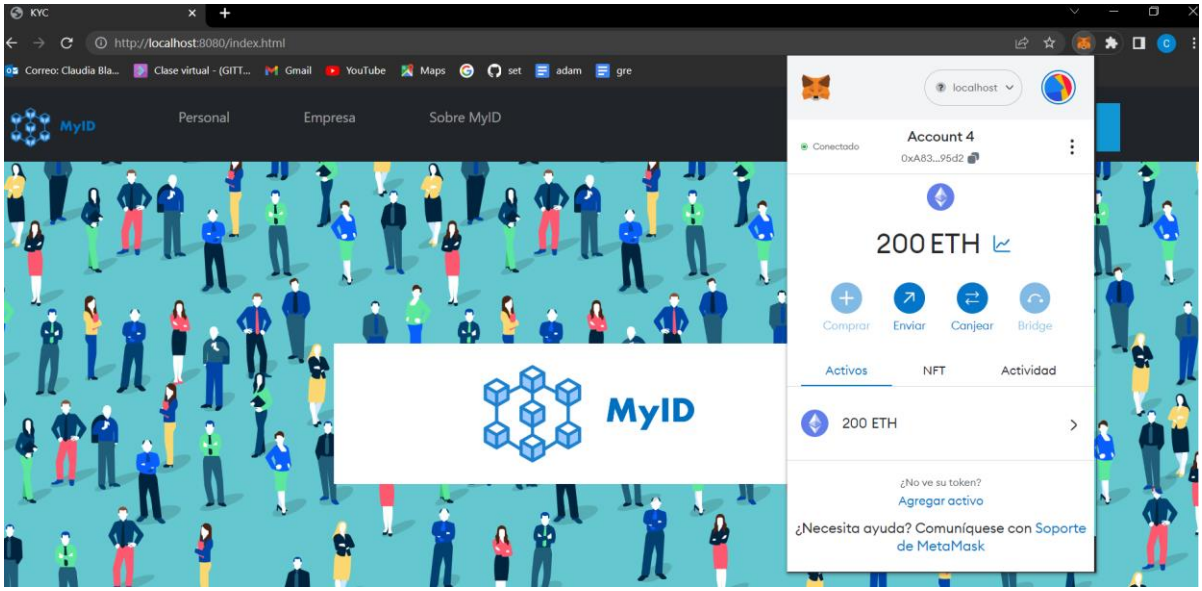


Ilustración 35: Ejemplo de uso de la extensión de MetaMask

El uso de *MetaMask* ha sido útil durante el desarrollo del proyecto para hacer pruebas de la aplicación. Pero también presenta muchas ventajas en el caso de uso real:

- Interfaz fácil de usar. *MetaMask* proporciona una interfaz de usuario intuitiva y amigable que permite a los usuarios gestionar fácilmente sus cuentas *Ethereum* y realizar transacciones en *Dapps* sin la necesidad de comprender los detalles técnicos subyacentes.
- Seguridad y control. Esta extensión de navegador almacena las claves privadas y las identidades digitales del usuario de forma segura en su dispositivo, proporcionando al usuario un mayor control sobre sus activos y su privacidad. Además, utiliza un enfoque de autenticación seguro para proteger las transacciones y las interacciones con *Dapps*.
- Conveniencia y portabilidad. Al utilizar *MetaMask*, los usuarios pueden acceder a sus cuentas y *Dapps* desde cualquier dispositivo o navegador compatible. Esto

permite una experiencia de usuario consistente y evita la necesidad de administrar múltiples *wallets* o claves privadas en diferentes plataformas.

7.1.4 SPRING BOOT

Se ha utilizado *Spring Boot* porque proporciona un modelo de configuración de aplicaciones de empresa basadas en *Java* para cualquier plataforma de despliegue (Spring Boot, 2023).

El *framework* que ofrece *Spring Boot* ha sido útil para el manejo de las bases de datos de usuarios y organizaciones, y también se ha usado para el *mock* de las APIs de ASNEF, CIRBE, Hacienda y el Ministerio del Interior.

La estructura que se ha seguido para todos estos casos se muestra a continuación.

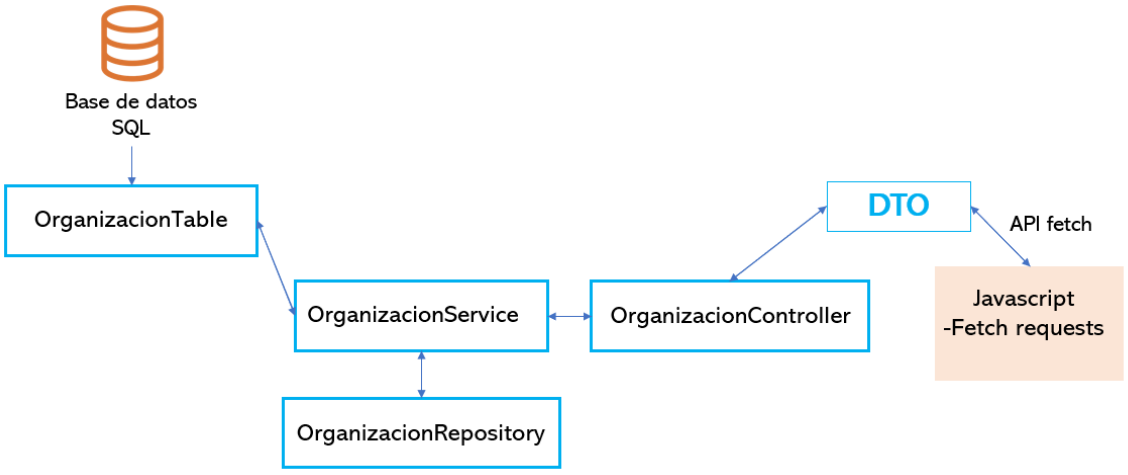


Ilustración 36: Framework de Spring Boot empleado

La clase *Table* permite interactuar fácilmente con la base de datos. El *Service* y el *Repository* incluyen funcionalidades por defecto otorgadas por el *framework* de *Spring Boot* que facilitan operaciones de obtención, actualización, inserción y eliminación de datos de la base de datos. El *Controller* usa estos servicios, y es la parte "visible" de la simulación de las APIs. El *DTO* (*Data Transfer Object*) sirve para transferir estructuras u objetos de datos entre los diferentes elementos descritos. Es especialmente relevante en el "cambio" de *JavaScript* a *Java* y viceversa.

Para la base de datos se ha utilizado H2, que integra una base de datos embebida en local. Se ha decidido utilizar este tipo de base de datos porque es sencilla de usar a la hora de hacer pruebas. Con el *framework* de *Spring Boot*, simplemente se necesitan dos ficheros de extensión *.sql* para definir la base de datos relacional y sus tablas: *schema.sql* y *data.sql*, respectivamente.

La base de datos tiene varias tablas:

- **Usuarios**. Incluye el nombre, DNI, correo electrónico, contraseña y nombre de usuario de los usuarios. No se ha incluido el *rating* o puntuación en esta tabla porque solo se debería poder obtener de *Blockchain*.
- **Organizaciones**. Incluye el nombre y la contraseña de cada organización registrada.
- **Documentos**. Incluye todos los documentos subidos al sistema por usuarios, además del *hash* de los mismos.

src > main > resources > schema.sql

```
-- SCHEMA

DROP TABLE IF EXISTS USUARIOS;
DROP TABLE IF EXISTS ORGANIZACIONES;
DROP TABLE IF EXISTS DOCUMENTOS;
DROP TABLE IF EXISTS USUARIOSCIRBE;

CREATE TABLE USUARIOS (
    ID INTEGER IDENTITY NOT NULL PRIMARY KEY,
    USER_NAME VARCHAR(255) NOT NULL,
    DNI VARCHAR(255) NOT NULL,
    USER_DATA VARCHAR(255) NOT NULL,
    USER_PWD VARCHAR(255) NOT NULL,
    USER_EMAIL VARCHAR(255) NOT NULL
);

CREATE TABLE ORGANIZACIONES (
    ID INTEGER IDENTITY NOT NULL PRIMARY KEY,
    ORG_NAME VARCHAR(255) NOT NULL,
    ORG_PWD VARCHAR(255) NOT NULL
);

CREATE TABLE DOCUMENTOS (
    ID INTEGER IDENTITY NOT NULL PRIMARY KEY,
    DNI VARCHAR(255) NOT NULL,
    DOCHASH VARCHAR(255) NOT NULL,
    DOCUMENT_DATA BLOB
);

```

Ilustración 37: Creación de tablas de la base de datos

La base de datos incluye cinco tablas más que se han usado para hacer el *mock* de las APIs que se describe en el próximo apartado.

- **Usuarios CIRBE**
- **Usuarios ASNEF**
- **Hacienda**
- **DNIS**
- **AEB**

7.1.5 MOCK DE APIS

Para el *mock* de las APIs mencionadas, ha sido útil utilizar *Postman*, una plataforma para crear y testear APIs (Postman, 2023). *Postman* ha permitido hacer pruebas de la estructura de *Spring Boot* de manera sencilla antes de integrarla con el *Front End* de la aplicación. Las APIs que se han simulado son: API CIRBE, API ASNEF, API Hacienda, API Ministerio de Interior y API AEB.

Una API (*Application Programming Interface*) actúa como intermediario en la transferencia de datos o información entre sistemas (IBM, 2023). El *payload* de una API está compuesto por esta serie de datos o información que se envía entre sistemas. Se pueden hacer diferentes tipos de peticiones a una API: GET, POST, PUT, DELETE… Estos métodos sirven para acceder a o modificar los datos de la API. Todas estas peticiones se han *mockeado* gracias a la estructura de *Spring Boot* explicada anteriormente.

El aspecto del *payload* de las APIs *mockeadas* en *Postman* se muestra en las siguientes ilustraciones.

Esta primera ilustración muestra la API del CIRBE y también la interfaz gráfica de *Postman*. Esta API devuelve entradas con números de DNI asociados a sus deudas, en euros. El CIRBE no tiene información sobre los pagos o impagos de estas.

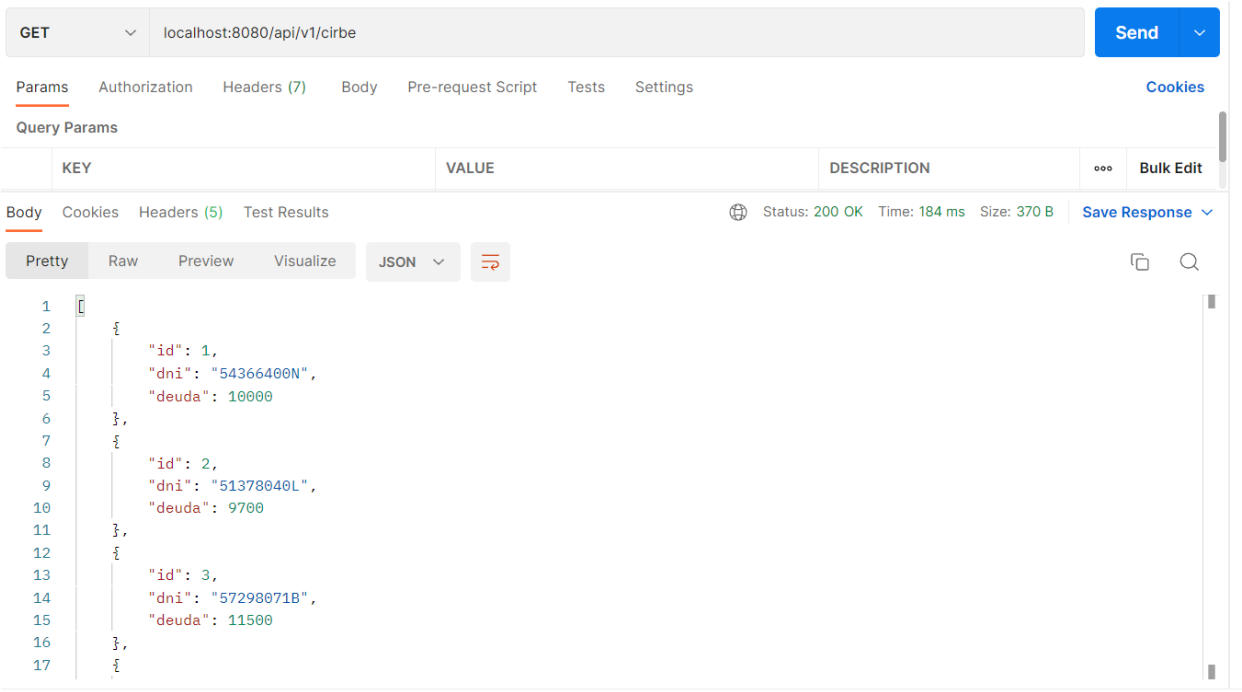


Ilustración 38: API CIRBE

La API del Ministerio del Interior devuelve entradas con números de DNI asociados al *hash* del PDF oficial de dichos documentos de identidad.


```
{
    "id": 2,
    "dni": "54366400N",
    "dniHash": "a975859739bc61068daaba88430994700aa6a487f351fc6f7630023e76d9e3c8"
}
```


Ilustración 24: API Ministerio del Interior

La API de ASNEF simplemente devuelve entradas con los números de DNI de individuos que están incluidos en el fichero ASNEF por incumplimiento de pagos o devolución de préstamos.

```
{
    "id": 1,
    "dni": "41294522T"
},
{
    "id": 2,
    "dni": "63829104X"
}
```


Ilustración 25: API ASNEF

Por otro lado, la API de Hacienda devuelve entradas con números de DNI asociados al *hash* del PDF oficial de la declaración de la renta del dueño de dicho cada DNI.


```
{
    "id": 1,
    "dni": "54366400N",
    "docHash": "6996994ed5ad2e50cf425b1f8dd10e3a39ba2d1cc42ee66f208f4935ba487ba3"
}
```


Ilustración 39: API Hacienda

Por último, la API de la Asociación Española de Banca (AEB) devuelve entradas con nombres de organizaciones asociados a un "código de verificación" que deben utilizar cuando se registren en la aplicación para confirmar su legitimidad.


```
{
    "id": 1,
    "orgName": "ZBank",
    "orgCode": "571onzk%cd"
},
{
    "id": 2,
    "orgName": "QBank",
    "orgCode": "623onib%qw"
},
```


Ilustración 40: API AEB

Como se ha mencionado anteriormente, el *mock* de estas APIs se ha llevado a cabo usando una base de datos H2 en el entorno de *Spring Boot* del proyecto.

En un contexto real, se necesitaría tener algún tipo de acuerdo con estas entidades o instituciones para poder tener acceso a toda esa información.

Capítulo 8. ANÁLISIS DE RESULTADOS

Los procesos KYC son esenciales para la verificación de identidades de clientes en entidades bancarias y para evitar problemas de blanqueo de capitales o falsificación de documentación. Son procesos costosos en términos temporales y económicos.

Muchas instituciones y entidades financieras o crediticias han digitalizado este proceso para hacerlo más conveniente y transparente, introduciendo el KYC electrónico. Esta digitalización les da flexibilidad a los usuarios, ya que pueden completar el proceso desde sus hogares de forma remota. Sin embargo, siguen siendo procesos costosos y siguen presentando algunos problemas, como la falta de una estandarización global, posibles actividades fraudulentas durante el proceso *online* y otras preocupaciones de privacidad (Hannan, Shahriar, Ferdous, Morshed Chowdhury, & Rahman, 2023). Estos problemas aún deben resolverse.

En este proyecto se ha desarrollado un modelo en el cual se agilizan algunos de los pasos comunes de los procesos KYC.

Para hacer un análisis de resultados en profundidad, en primer lugar, se muestran las tareas de la planificación inicial del proyecto y los detalles de su cumplimiento.

Tarea	**Cumplimiento**
Definición del proyecto	La definición y el planteamiento del trabajo se han realizado de manera satisfactoria, tal y como se explica en el Definición del Trabajo. Se han añadido ciertos puntos respecto al planteamiento inicial del proyecto.

Investigación y documentación de la tecnología *Blockchain*	Se ha estudiado la tecnología y se ha podido aplicar durante el desarrollo del proyecto.
Investigación sobre identidades digitales e identidades basadas en *Blockchain*	Se han estudiado los puntos clave de las identidades digitales actuales y se han identificado ejemplos de uso de *Blockchain* en la verificación de identidades, como se explica en el Estado de la Cuestión.
Investigación sobre procesos KYC y *scoring* crediticio en entidades bancarias	Se ha investigado sobre diferentes tipos de procesos KYC, el mercado del KYC electrónico y los sistemas de *scoring* que utilizan entidades bancarias españolas, tal y como se explica en el Estado de la Cuestión.
Aprendizaje de *Solidity*	Se ha aprendido a manejar *Solidity* y a programar *Smart Contracts* con soltura.
Estudio de *Ganache* y *MetaMask*	Se ha aprendido a utilizar *Ganache* y se ha podido crear una red de pruebas de *Ethereum* en local a la que conectarse usando la cartera o *wallet* de *MetaMask*.
Estudio de *JavaScript* y *Web3.js*	Se han integrado de forma satisfactoria los conocimientos previos de *JavaScript* con los nuevos de la librería *Web3.js.*
Estudio del entorno de desarrollo	Se ha aprendido a manejar la extensión de *Ethereum Remix* en el editor de código *Visual Studio Code.*
Desarrollo del proyecto	80

Redacción de la memoria	Se ha redactado la memoria en varias partes. En la etapa inicial del proyecto, durante la investigación, se escribieron los primeros seis capítulos. El resto se han ido escribiendo durante el desarrollo y tras acabar este.
Revisión de la memoria y posibles cambios	Se ha revisado la memoria y se han hecho los cambios necesarios.
Elaboración de la presentación	Se ha elaborado una presentación del proyecto, además de un vídeo-demo para mostrar más claramente sus funcionalidades.

Ilustración 41: Tareas realizadas con comentarios

Como muestra la tabla anterior, se han realizado con éxito las tareas de la planificación y solo se han introducido algunos cambios menores durante el desarrollo del proyecto. En definitiva, el resultado de la planificación ha sido satisfactorio.

8.1 IDENTIDAD DIGITAL FINANCIERA BASADA EN BLOCKCHAIN

El proyecto ha logrado con éxito crear una identidad financiera digital basada en la tecnología *Blockchain*. Se ha desarrollado un sistema que otorga a los usuarios una identidad personal, segura e inmutable basada en información social y económica/crediticia. Además, esta identidad es verificada en varios puntos, siendo *Blockchain* el punto principal para su legitimidad y transparencia.

La creación de esta identidad financiera digital basada ha sido un logro destacado en el campo de las finanzas. Sin embargo, es esencial examinar de manera crítica y realista esta

identidad desarrollada para poder identificar tanto sus aspectos positivos como sus limitaciones.

En primer lugar, es importante destacar los beneficios de esta identidad financiera digital. Proporciona a los individuos una forma confiable de gestionar sus actividades financieras, especialmente en el ámbito de los créditos y los préstamos. Como se ha explicado anteriormente, gracias a la tecnología *Blockchain*, la identidad de los usuarios se encuentra protegida de manera segura y se verifica en múltiples puntos, lo que contribuye a la legitimidad y transparencia de las transacciones financieras.

Además, esta identidad financiera digital ofrece una mayor autonomía y control a los individuos. Al tener acceso a su propia identidad, los usuarios pueden tomar decisiones informadas y gestionar su historial crediticio de manera más efectiva. Esto puede ser especialmente útil para aquellos que buscan obtener préstamos, ya que contar con una identidad financiera confiable puede aumentar sus posibilidades de obtener mejores condiciones para los mismos.

No obstante, es importante tener en cuenta que esta identidad financiera digital no es una solución completa para todos los aspectos de la identidad personal. Si bien es valiosa en el ámbito de los créditos y las finanzas, no aborda otros aspectos cruciales de la identidad, como la identidad civil o la identificación legal. Por lo tanto, es importante reconocer sus limitaciones y no considerarla como una identidad integral.

También es necesario tener en cuenta los desafíos y obstáculos que pueden surgir en la implementación y adopción de esta identidad financiera digital basada en *Blockchain*. Aunque la tecnología *Blockchain* ofrece seguridad y transparencia, existen preocupaciones en torno a la privacidad y la protección de datos personales. Garantizar la protección de la información sensible y abordar posibles vulnerabilidades de seguridad es fundamental para fomentar la confianza y la aceptación de esta identidad financiera.

8.2 MAYOR EFICIENCIA Y SEGURIDAD EN PROCESOS KYC

Durante el registro, el *hash* del DNI oficial del usuario queda guardado en *Blockchain*. Además, para su verificación se usa una API de forma directa.

Para los clientes, es más sencillo y rápido verificar su identidad. La API del Ministerio de Interior verifica la identidad del usuario de forma directa, lo que elimina algunos pasos de los procesos KYC tradicionales, mostrados en la Ilustración 6: Proceso KYC tradicional presencial (Klippa, 2022) y en la Ilustración 7: Proceso KYC tradicional online (Klippa, 2022).

En los procesos KYC *online* tradicionales, se debe hacer una comprobación de los documentos que proporciona el cliente, y en muchos casos se debe hacer también un monitoreo posterior. Además de tener asociado un coste temporal y económico elevado, las comprobaciones pueden pasar por alto ciertos indicadores de problemas de seguridad. Con la solución propuesta por el proyecto, esto no ocurre porque se pueden hacer comprobaciones dobles, en la *Blockchain* y en la API oficial del Ministerio del Interior. No solo las comprobaciones son dobles, sino que también las actualizaciones lo son.

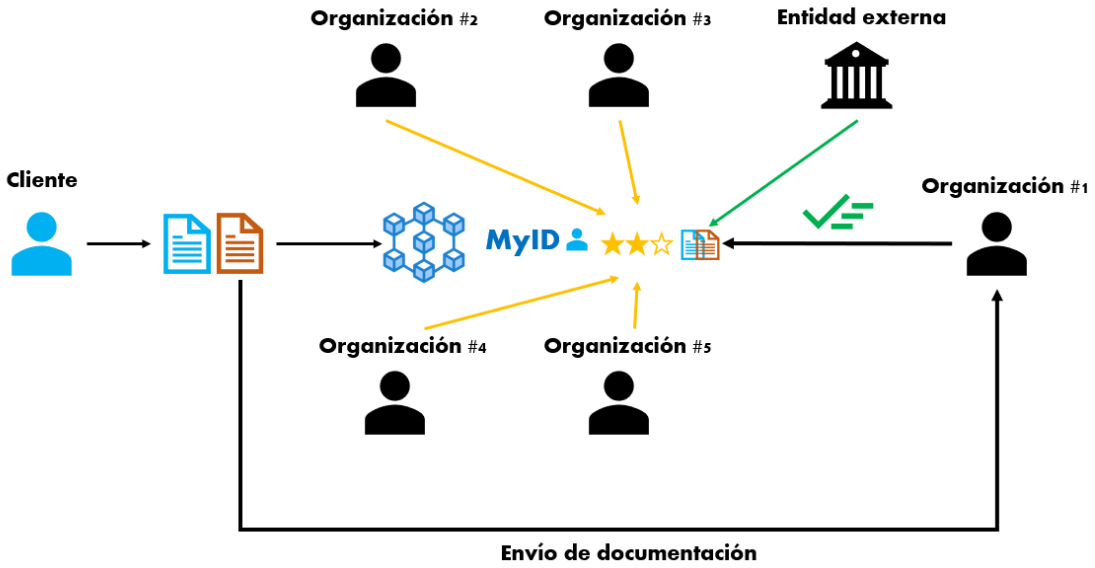


Ilustración 42: Esquema de nuevo proceso KYC propuesto

Como se muestra en la Ilustración 42: Esquema de nuevo proceso KYC propuesto, el modelo propuesto mejora la eficiencia del proceso KYC tradicional.

- Se sigue requiriendo un envío de documentación, pero la verificación por parte de las organizaciones no implica tantas comprobaciones manuales, ya que la misma red de *Ethereum* verifica la identidad del usuario cuando este se registra, por lo que está implícitamente comprobada. Además, las verificaciones que las organizaciones suelen hacer a través de otras entidades externas ya no son necesarias al estar incluidas en la aplicación y verificadas en la red de *Ethereum*.
- La organización no necesita hacer comprobaciones adicionales para su propio modelo de *scoring* bancario porque el DNI del usuario está asociado a su *rating* en MyID que refleja su comportamiento financiero o crediticio, y está respaldado por otras organizaciones legítimas.
- Respecto a los procesos KYC tradicionales, se aumenta el número de entidades que participan en la verificación KYC de forma transparente, respetando la privacidad del usuario al estar su DNI asociado a su *rating* sin datos adicionales en *Blockchain*. Se asegura la legitimidad de las organizaciones durante el proceso de registro en la plataforma de las mismas, haciendo uso de nuevo de la información aportada por una entidad externa, la Asociación Española de Banca. Además, se otorga más capacidad de *rating* a aquellas organizaciones con mayor puntuación. De ese modo la red queda asegurada.
- El proceso de verificación es más sencillo para los usuarios o clientes, ya que utilizan la identidad que les proporciona la red de *Ethereum* para identificarse en los procesos KYC y para actualizar su documentación si es necesario.

8.3 INDICADORES DE PROBLEMAS DE SEGURIDAD

Blockchain mantiene un registro inmutable de transacciones que es muy difícil de modificar, a diferencia de otros sistemas de "almacenamiento" como las bases de datos tradicionales, que también se han empleado en este proyecto.

Al contar con dos puntos de comprobación y actualización, como se ha explicado en el apartado anterior, un cambio en la base de datos que no está reflejado en *Blockchain* puede indicar un problema de seguridad o falsificación, por lo que es más sencillo detectar este tipo de problemas.

A continuación, se ilustra un ejemplo de caso de indicador de un problema de seguridad que permitiría detectar algún tipo de *hackeo*.

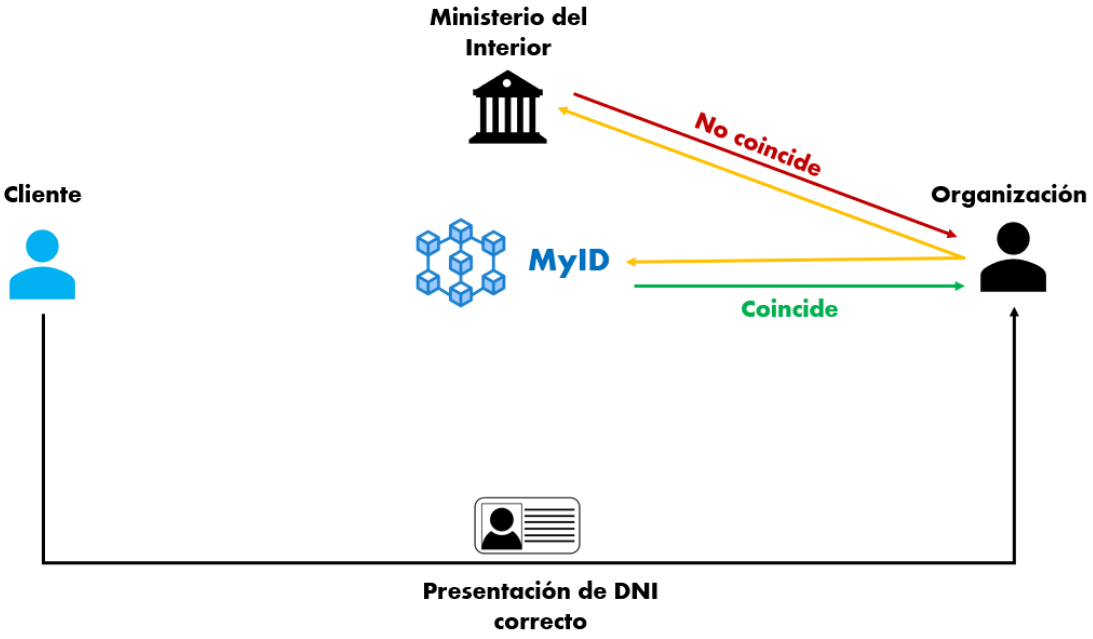


Ilustración 43: Ejemplo de posible brecha de seguridad

En el ejemplo anterior, el cliente presenta a la organización en la que quiere solicitar un crédito o un préstamo su DNI oficial y real, que está correctamente referenciado en la red de *Blockchain* de MyID. La organización lleva a cabo la verificación del documento

proporcionado por el cliente, que se trata de una verificación en dos puntos, como se ha mencionado anteriormente:

- Verificación en *Blockchain*. El DNI es correcto y coincide con el referenciado en *Blockchain*.
- Verificación en la API externa del Ministerio del Interior. Aunque el DNI es correcto, no coincide con el referenciado en la API mencionada.

Cuando un cliente sube un documento, ya sea al registrarse (cuando sube el DNI) o al actualizarlo, siempre se verifica con dicha API antes. Si ahora no coincide, esto puede estar causado por una razón principal:

- Brecha de seguridad en la API del Ministerio del Interior. Se ha modificado el contenido de la base de datos del Ministerio del Interior o se ha comprometido la seguridad de la API.

El procedimiento de detección de brechas de seguridad sería similar para el caso de la API de la Agencia Tributaria.

8.4 PORTABILIDAD DE LA APLICACIÓN

La aplicación propuesta por el proyecto puede ser portátil y compatible con diferentes plataformas y servicios, lo que permite su integración con diversas organizaciones. Un ejemplo de ello es el uso de la *wallet* de *MetaMask*, la billetera digital para criptomonedas y *tokens*, que puede ser aprovechada por las organizaciones para facilitar el acceso y la interacción con la aplicación.

La *wallet* de *MetaMask* ofrece una solución segura y conveniente para gestionar activos digitales y realizar transacciones en la *Blockchain*. Al permitir a las organizaciones almacenar y controlar sus claves privadas, la billetera garantiza la seguridad de los fondos y proporciona una forma fácil de acceder a diferentes servicios y aplicaciones basados en criptomonedas.

Además, esta *wallet* se integra en diferentes navegadores y dispositivos, lo que implica una mayor accesibilidad y portabilidad de la aplicación para las organizaciones, permitiendo que estas utilicen la aplicación de manera conveniente. Se trata, por tanto, de una aplicación compatible con una amplia variedad de entornos de navegación *online*.

La *wallet* se usa en diferentes puntos de operación del sistema desarrollado.

Por ejemplo, una institución financiera puede utilizar la *wallet* para autenticarse en la web y poder buscar el DNI de un cliente y acceder a su historial crediticio y financiero almacenado en la aplicación.

La aplicación también accederá a la dirección o *address* de la organización a través de la *wallet* de *MetaMask* para verificar la puntuación o *rating* de esta cuando intente acceder a ciertas funcionalidades. Por ejemplo, una organización con puntuación inferior a 8 no podrá acceder a la información de las APIs externas. Otro ejemplo es que las organizaciones con puntuación superior a 6 tienen la opción de otorgar más votos a los clientes o usuarios, a diferencia de las organizaciones con puntuación inferior a 6.

8.5 ANÁLISIS CRÍTICO DE LOS RESULTADOS

Aunque la solución propuesta soluciona algunos de los problemas de los procesos KYC, y simultáneamente logra cumplir los objetivos iniciales del proyecto, aún quedan algunos puntos por resolver o mejorar.

La aplicación propuesta ofrece un sistema de identidad crediticia muy completo que aborda los desafíos clave de los procesos KYC. Sin embargo, es importante tener en cuenta que también depende de entidades externas para recopilar y verificar la información necesaria. Esto refleja claramente la necesidad de mantener algunos de los aspectos tradicionales de los procesos KYC, en los cuales las instituciones financieras y otras organizaciones confían en fuentes de datos externas para obtener información precisa y actualizada sobre los clientes.

La dependencia de entidades externas puede ser tanto una ventaja como una limitación. Por un lado, permite acceder a una amplia gama de datos financieros y de crédito que son esenciales para construir una identidad crediticia sólida. Al utilizar fuentes externas confiables, como informes de crédito y bases de datos financieros, la aplicación puede proporcionar a las organizaciones una visión completa del historial crediticio y la solvencia de sus clientes.

Sin embargo, por otro lado, esta dependencia también puede presentar ciertos problemas. La calidad y disponibilidad de los datos externos pueden variar según la región y las fuentes utilizadas. Además, algunas entidades pueden tener políticas de privacidad y protección de datos que dificulten el acceso a sus datos y la recopilación de información. Estos problemas pueden afectar la precisión y confiabilidad de la identidad crediticia generada por la aplicación.

Además, es importante destacar que la identidad personal no se limita únicamente a los aspectos financieros y de crédito. Para obtener una identidad completa y precisa, también se requiere una variedad de datos adicionales, como información personal, educativa, laboral y de historial médico, entre otros. Estos datos adicionales pueden ser clave para evaluar la solvencia de una persona en contextos específicos, como la concesión de préstamos para educación, vivienda o servicios médicos.

Aunque el alcance del proyecto se ha limitado a los aspectos financieros y de crédito de la identidad, es importante reconocer la necesidad de considerar estos otros aspectos en futuros desarrollos. La recopilación y gestión de datos personales adicionales plantea desafíos significativos en términos de privacidad y seguridad, así como de cumplimiento normativo. Estos desafíos podrían requerir una mayor colaboración con otras entidades y la implementación de medidas adicionales de protección de datos.

Por último, en cuanto a temas de seguridad de la aplicación, podría ocurrir un “Spam de Creación de Cuentas” de organizaciones: un único actor fraudulento podría crear miles de cuentas falsas para propagar su operación al resto del sistema (Xiao, Freeman, & Hwa, 2015). En el siguiente capítulo se explicarán los trabajos y cambios futuros necesarios para

evitar este problema que no se han desarrollado en este proyecto por falta de recursos temporales, principalmente. Se debe tener en cuenta que este no ha sido el enfoque principal del proyecto.

Capítulo 9. CONCLUSIONES Y TRABAJOS FUTUROS

Se ha logrado alcanzar los objetivos iniciales del proyecto con éxito. La siguiente tabla describe el grado de cumplimiento de los objetivos que se plantearon al comienzo del proyecto.

Objetivo	**Cumplimiento**
Agilización de procesos KYC. Crear una aplicación que haga los procesos de identificación digital más eficientes, que esté disponible para cualquier persona y que proporcione a los usuarios una identidad digital segura, fiable y controlada por ellos mismos.	La aplicación propone un modelo que agiliza los procesos KYC, tanto en el lado de cliente como en el lado de entidad u organización, como se ha explicado en el Mayor eficiencia y seguridad en procesos KYC.
Identidad financiera o crediticia digital. Proporcionar al usuario una identidad financiera digital respaldada por datos socioeconómicos y basada en *Blockchain* que le permita demostrar ciertos datos de su identidad (especialmente datos económicos para adquirir créditos) de manera irrefutable.	El proyecto ha desarrollado una identidad financiera digital para los usuarios o clientes, basada principalmente en sus datos crediticios.
Aplicación web. Crear un ejemplo de caso de uso en una aplicación web que muestre la solución propuesta por el proyecto.	Se ha creado un ejemplo de caso de uso en una aplicación web utilizando las tecnologías descritas en el Descripción de las Tecnologías.

Tabla 8: Cumplimiento de los objetivos del proyecto

Se ha concluido que la identidad de una persona cuenta con múltiples componentes e integrarlas en una única identidad supone un reto. Inicialmente, el proyecto planteó la idea de crear una identidad que englobara tanto datos financieros como datos de carácter social, como títulos educativos o permisos de conducir de los usuarios. Sin embargo, se ha decidido limitar el alcance del proyecto únicamente a los aspectos financieros. Esta decisión se tomó debido a los desafíos técnicos y de privacidad que implicaría la integración de demasiados datos sociales en una única identidad digital. Al enfocarse exclusivamente en aspectos financieros, se busca garantizar la seguridad y confidencialidad de la información de los usuarios.

La proliferación de múltiples identidades digitales ha demostrado ser problemática, generando riesgos como *hackeos* de diferentes cuentas y preocupaciones relacionadas con la privacidad de los datos (Rodrigues, 2015). La solución ideal consiste en encontrar un equilibrio, y es aquí donde *Blockchain* y su seguridad y transparencia desempeñan un papel fundamental.

También cabe destacar que la tecnología *Blockchain*, a pesar de una caída en su uso y popularidad después de 2018, continúa evolucionando, y a medida que avanza, sus posibles usos siguen ampliándose (Ahrens, 2023). La industria de las finanzas es en la que más extendido está el uso de esta tecnología, pero se está extendiendo a muchos otros sectores (Marley, 2021).

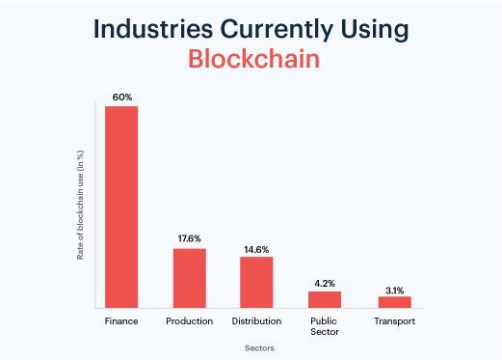


Ilustración 44: Industrias que usaban Blockchain en 2021 (Marley, 2021)

Este proyecto puede servir como base para otros más evolucionados, como se explicará en más detalle en la siguiente sección. A medida que la tecnología *Blockchain* avance, es muy probable que surjan nuevas oportunidades y soluciones innovadoras en el ámbito de la identidad digital y la gestión de datos financieros. Este proyecto actual sienta las bases para futuros desarrollos que pueden aprovechar las mejoras y avances en la tecnología *Blockchain*, lo que permitiría perfeccionar aún más la seguridad, la privacidad y la eficiencia de los procesos KYC de identificación y verificación financiera.

9.1 TRABAJOS FUTUROS

En cuanto a los trabajos futuros, se plantean diferentes posibilidades para el proyecto. Para empezar, se hace un breve análisis de posibles medidas de seguridad a implementar. También se mencionan proyectos de otros ámbitos que podrían utilizar la aplicación desarrollada como base.

9.1.1 MEDIDAS DE SEGURIDAD

Uno de los principales desafíos de seguridad que podría presentar la aplicación el Spam de Creación de Cuentas. Esto refiere a la generación masiva de cuentas falsas o no deseadas con el fin de inundar y saturar los sistemas y servicios de una aplicación *online*. Se proponen, como trabajos futuros, varias soluciones:

- **Uso de CAPTCHA** (*Completely Automated Public Turing test to tell Computers and Humans Apart*). Esto ayudaría a diferenciar a los humanos de los *bots* al presentar desafíos visuales o de audio que solo pueden ser resueltos por humanos, protegiendo así la aplicación contra actividades maliciosas automatizadas.
- **Bloqueo de direcciones IP**. Esto implicaría prohibir el acceso a un sistema o servicio en línea desde una dirección IP específica desde la que se creen demasiadas cuentas en la aplicación, con el objetivo de mitigar el spam y proteger la integridad y calidad del sistema.
- **Algoritmos de aprendizaje automático o *Machine Learning***. Este tipo de algoritmos ayudaría a distinguir las cuentas legítimas de las cuentas de spam.

9.1.2 ACUERDOS Y CONEXIONES CON ENTIDADES EXTERNAS

La aplicación necesita establecer conexiones con entidades como el Ministerio del Interior y el CIRBE para poder acceder a los datos de sus clientes para los procesos de verificación KYC. En el proyecto se han simulado o *mockeado* estas conexiones a través de APIs, pero en un entorno real deberían establecerse ciertos acuerdos legales para que la aplicación pueda acceder a los datos de estas entidades.

La aplicación también debería cumplir con los cambios establecidos en la Norma UNE 71307-1 de España, publicada por la Asociación Española de Normalización (UNE). Esta norma, que representa el primer estándar europeo en la gestión de identidades digitales descentralizadas basadas en *Blockchain*, proporciona un marco de referencia genérico para la emisión, administración y uso de identidades digitales autogestionadas, lo que garantiza seguridad y protección de la privacidad en los procesos (Vanci, 2021). La norma establece requisitos técnicos y de seguridad que deben cumplir las soluciones de identidad digital descentralizadas basadas en *Blockchain*. Esto incluye aspectos como la autenticación, la integridad de los datos, la protección de la privacidad, la gestión de claves y certificados, y la interoperabilidad entre diferentes sistemas y plataformas.

9.1.3 AMPLIACIÓN A INSTITUCIONES EDUCATIVAS Y EMPRESAS

Una identidad digital basada en *Blockchain* tiene el potencial de ser ampliada y aplicada en instituciones educativas y empresas. Al extender este proyecto a estas áreas, es posible utilizar la tecnología *Blockchain* para verificar títulos universitarios en procesos de selección para puestos en empresas, lo que podría agilizar y simplificar los procesos de contratación. Sin embargo, también es importante considerar las ventajas y desventajas que esto puede causar.

Una de las principales ventajas de esta ampliación es que podría ayudar a reducir la falsificación de títulos y garantizar una mayor confianza en la información presentada por los postulantes. Además, al utilizar una identidad digital basada en *Blockchain*, se podría agilizar y simplificar el proceso de verificación de antecedentes y referencias laborales. Las

empresas podrían acceder de manera segura a la información pertinente sobre la experiencia y las calificaciones de los candidatos, lo que permitiría una toma de decisiones más informada y eficiente durante el proceso de selección.

Sin embargo, también es necesario considerar las desventajas y desafíos de este enfoque. Uno de los principales problemas es la desigualdad social que podría causar. La implementación de este sistema puede excluir a aquellos individuos que no tienen acceso a una educación formal o que no pueden permitirse los costes asociados con la obtención de títulos universitarios. Esto podría ampliar la brecha social entre aquellos que pueden permitirse una educación superior, y por tanto demostrar sus credenciales fácilmente, y aquellos que no tienen la misma oportunidad.

9.1.4 VERIFICACIÓN DE EDAD EN DIFERENTES ÁMBITOS

El proyecto también se podría ampliar a la verificación de edad en diferentes ámbitos. Este proceso de verificación es muy similar a los procesos KYC que realizan las entidades bancarias, pero es incluso más sencillo.

Una identidad digital basada en *Blockchain* permitiría a los usuarios verificar su edad de manera más eficiente. Algunos ejemplos de casos de uso de esta verificación de edad utilizando *Blockchain* son:

- **Alquiler de vehículos**. En España, la edad mínima para alquilar un coche es de 21 años. Sería sencillo alquilar un coche desde otra parte del mundo o del país si se puede verificar la edad *online*. También se podría acceder a los datos del permiso de conducir del usuario si se usase una API de la Dirección General de Tráfico (DGT), usando como base el sistema que se ha desarrollado para acceder a la información de las entidades como el CIRBE o ASNEF.
- **Venta de productos restringidos**. La verificación de edad también es común en la venta de productos como bebidas alcohólicas o tabaco. Una verificación basada en *Blockchain* haría más segura la compra de estos productos, especialmente dada la

popularidad de aplicaciones de entrega a domicilio que también envían este tipo de productos.

- **Eventos y espectáculos**. Muchos festivales, discotecas y eventos tienen restricciones de edad. Las comprobaciones de edad de los asistentes requieren un elevado coste temporal, especialmente en eventos de grandes aforos, además de suponer un coste de personal.

El proyecto podría servir de base para otro más evolucionado que incluyera la edad de los usuarios como parte del proceso general de verificación de información.

9.1.5 AMPLIACIÓN A OTRAS INDUSTRIAS QUE USAN KYC

Este proyecto también podría servir como base para procesos KYC en diferentes ámbitos. Muchas entidades requieren estos procesos. A continuación, se presentan dos ejemplos específicos:

- **Compañías de seguros.** En el caso de incluir datos médicos en la identidad descentralizada, este sistema podría resultar muy beneficioso para las compañías de seguros. Al contar con un proceso KYC basado en una identidad descentralizada, las compañías podrían verificar de manera eficiente y segura la autenticidad de los datos médicos proporcionados por los solicitantes de seguros. Esto permitiría una evaluación más precisa de los riesgos asociados y facilitaría el proceso de emisión de pólizas, agilizando así los trámites, reduciendo costes y mejorando la experiencia del cliente.
- **Sector de las telecomunicaciones.** Dado el crecimiento de la banca móvil, este sistema sería también muy útil en el sector de las telecomunicaciones (Ketkar, Shankar, & Banwet, 2014). La banca móvil se considera un medio efectivo para mejorar la inclusión financiera y, como resultado, existe una necesidad de alinear los procesos KYC del sector de las telecomunicaciones con los de la banca. Mediante el uso de una identidad descentralizada basada en *Blockchain*, las empresas de telecomunicaciones podrían verificar la identidad de sus clientes de manera segura y

confiable, cumpliendo así con los requisitos regulatorios y brindando servicios más seguros.

Capítulo 10. BIBLIOGRAFÍA

Ahrens, B. (2 de febrero de 2023). *Crypto*. Obtenido de Plug and Play: https://www.plugandplaytechcenter.com/resources/Blockchain-stocks-evolution-of-Blockchain-technology/#:~:text=Today%2C%20the%20technology%20is%20used,potential%20uses%20are%20only%20growing.

Applicantes. (11 de mayo de 2023). *El 86% de los usuarios españoles ya utiliza apps de banca tradicional*. Obtenido de Applicantes: https://applicantes.com/apps-bancos-adopcion/#:~:text=El%2086%25%20de%20los%20usuarios%20espa%C3%B1oles%20ya%20utiliza%20apps%20de%20banca%20tradicional,-applicantes%20%7C%2011%20mayo&text=No%20hace%20demasiado%20que%20realizar,y%20recelo%2C%20e%20incluso

ASNEF. (2023). *Fichero Asnef.* Obtenido de ASNEF: https://asnef.com/fichero-asnef/preguntas-frecuentes/

Australia Post. (2023). *Apply for a Keypass ID*. Obtenido de Australia Post: https://auspost.com.au/id-and-document-services/apply-for-a-keypass-id

Bai, Y., Lei, H., Li, S., Gao, H., Li, J., & Li, L. (2022). Decentralized and Self-Sovereign Identity in the Era of Blockchain: A Survey. *IEEE International Conference on Blockchain.*

BBVA. (s.f.). *BBVA.* Obtenido de https://www.bbva.es/finanzas-vistazo/ef/prestamos/scoring-concesion-prestamo.html

ClearPay. (s.f.). *clearpay*. Obtenido de clearpay: https://www.clearpay.com/es-ES

Ethereum. (14 de enero de 2023). *Consensus Mechanisms*. Obtenido de Ethereum: https://ethereum.org/en/developers/docs/consensus-mechanisms/

Facts & Factors. (3 de mayo de 2023). *Global E-KYC Market Share Is Expected To Grow At A CAGR Of 21.55% By 2030*. Obtenido de Facts & Factors: https://www.fnfresearch.com/news/global-e-kyc-market

Ganache. (s.f.). Obtenido de Oreilly: https://www.oreilly.com/library/view/Blockchain-quick-start/9781789807974/9134ee72-d1a3-42ad-82c3-38d3f2fb8aa8.xhtml#:~:text=Ganache%20is%20a%20private%20Ethereum,Provides%20advanced%20mining%20control

Hannan, M. A., Shahriar, M. A., Ferdous, M. S., Morshed Chowdhury, M. J., & Rahman, M. S. (2023). A systematic literature review of Blockchain-based e-KYC systems. *Computing*.

Hussey, M., & Phillips, D. (9 de mayo de 2022). *¿Qué es MetaMask? Cómo Utilizar la Mejor —Y Más Popular— Wallet de Ethereum*. Obtenido de Decrypt: https://decrypt.co/es/resources/que-es-metamask-como-utilizar-la-mejor-y-mas-popular-wallet-de-ethereum

IBM. (2023). *What is an API?* Obtenido de IBM: https://www.ibm.com/topics/api

IEEE. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. *17th International Symposium INFOTEH-JAHORINA (INFOTEH)*. East Sarajevo.

Kapsoulis, N., Psychas, A., Palaiokrassas, G., Marinakis, A., Litke, A., & Varvarigou, T. (2020). Know Your Customer (KYC) Implementation with Smart Contracts on a Privacy-Oriented Decentralized Architecture. *MDPI*.

Ketkar, S. P., Shankar, R., & Banwet, D. K. (2014). Telecom KYC and mobile banking regulation:. *Journal of Banking Regulation*, 117-128.

Klippa. (16 de febrero de 2022). *How KYC automation can transform your business*. Obtenido de Klippa: https://www.klippa.com/en/blog/information/kyc-automation/

Marley, R. (1 de abril de 2021). *6 Upcoming trends in Blockchain and Cryptocurrency for 2021*. Obtenido de ShuftiPro: https://shuftipro.com/blog/6-upcoming-trends-in-Blockchain-and-cryptocurrency-for-2021/

Marous, J. (13 de Abril de 2021). *The Financial Brand.* Obtenido de https://thefinancialbrand.com/news/loan-growth/digital-banking-account-opening-sales-growth-112423/

McKinsey & Company. (5 de Octubre de 2020). *How COVID-19 has pushed companies over the technology tipping point—and transformed business forever*. Obtenido de McKinsey: https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever#/

MetaMask. (2023). *Access a user's accounts*. Obtenido de MetaMask: https://docs.metamask.io/wallet/get-started/access-accounts/

Nacional Credit. (23 de Febrero de 2023). *Nacional Credit.* Obtenido de https://www.nacionalcredit.es/que-deuda-hay-que-tener-para-aparecer-en-cirbe/

Naciones Unidas. (s.f.). *Objetivos de desarrollo sostenible*. Obtenido de Naciones Unidas: https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Obtenido de Bitcoin: https://bitcoin.org/bitcoin.pdf

Ondato. (2022). *The real cost of KYC & AML compliance for the financial sector.*

Postman. (2023). *About Postman*. Obtenido de Postman: https://www.postman.com/company/about-postman/

Research and Markets. (2023). *Spain Buy Now Pay Later Market.* Spain.

Rodrigues, R. (2015). Competencia Informacional, identidad digital y privacidad de datos: retos y desafíos que nos trae internet hoy. *Repositorio Institucional Universidad Centroamericana*, 3-4.

Singhal, N., Sharma, M. K., Samant, S. S., Goswami, P., & Abhilash, Y. (2020). Smart KYC Using Blockchain and IPFS. En V. K. Gunjan, S. Senatore, A. Kumar, X.-Z. Gao, & S. Merugu, *Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies* (págs. 77-84). Springer. doi:https://doi.org/10.1007/978-981-15-3125-5_9

Smith, O. (24 de febrero de 2020). *How Artificial Intelligence is Revamping KYC and AML?* Obtenido de Medium: https://medium.com/shufti-pro/how-artificial-intelligence-is-revamping-kyc-and-aml-f4b1538d5bc0

Solidity. (2016). *Expresiones y estructuras de control*. Obtenido de Solidity: https://solidity-es.readthedocs.io/es/latest/control-structures.html

Solidity. (s.f.). *Contract ABI Specification.* Obtenido de https://docs.soliditylang.org/en/v0.8.19/abi-spec.html

Solidity. (s.f.). *Solidity.* Obtenido de https://docs.soliditylang.org/en/v0.8.19/

Spring Boot. (2023). *Spring Framework.* Obtenido de Spring Boot: https://spring.io/projects/spring-framework

Thomason, J. (2021). Blockchain for Growth: Applying DLTs to the UN Sustainable Development Goals. En E. Kaili, & E. Psarrakis, *Disintermediation Economics* (págs. 93-110). Palgrave Macmillan.

Tyagi, N. K., Goyal, M., & Kumar, A. (2022). Game Theory-Based Proof of Stake Mining in Blockchain for Sustainable Energy Efficiency. *International Conference on Artificial Intelligence and Sustainable Engineering* (págs. 121-132). Singapore: Springer.

Vanci, M. (11 de enero de 2021). *España publica la primera norma sobre identidad digital basada en Blockchains.* Obtenido de CRIPTONOTICIAS: https://www.criptonoticias.com/regulacion/espana-publica-primera-norma-identidad-digital-basada-Blockchains/

Web3js. (s.f.). *web3.js - Ethereum JavaScript API*. Obtenido de Web3js: https://web3js.readthedocs.io/en/v1.8.2/

What is Java Spring Boot? (s.f.). Obtenido de IBM: https://www.ibm.com/topics/java-spring-boot

World Bank Group. (21 de julio de 2022). *COVID-19 Boosted the Adoption of Digital Financial Services*. Obtenido de The World Bank: https://www.worldbank.org/en/news/feature/2022/07/21/covid-19-boosted-the-adoption-of-digital-financial-services

Worldpay. (2022). *The global payments report.* FIS.

Xiao, C., Freeman, D. M., & Hwa, T. (2015). Detecting Clusters of Fake Accounts in Online Social Networks. *Proceedings of the 8th ACM Workshop on Artificial Intelligence and Security.*, (págs. 91-101). Denver.

Zhang, X., & Yin, Y. (2019). Research on Digital Copyright Management System Based on Blockchain Technology. *IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC).* Chengdu.

ANEXO I: ALINEACIÓN DEL PROYECTO CON LOS ODS

Los Objetivos del Desarrollo Sostenible fueron aprobados por la ONU en 2015 como parte de la Agenda 2030 sobre el Desarrollo Sostenible (Naciones Unidas, s.f.). Entre estos 17 objetivos están el fin de la pobreza, la igualdad de género y la lucha contra el cambio climático.

Ilustración 45: Objetivos de desarrollo sostenible (Naciones Unidas, s.f.)

Este proyecto de identidad financiera digital basada en *Blockchain* puede alinearse con varios ODS.

ODS 1: Fin de la pobreza

Al proporcionar una identidad financiera digital basada en *Blockchain*, el proyecto podría contribuir a mejorar el acceso a servicios financieros para personas en situación vulnerable o de pobreza. Esta aplicación les permitiría participar de manera más sencilla en

transacciones financieras, ahorrar y acceder a servicios básicos de crédito y préstamos, lo que ayuda a reducir la pobreza y fomentar la inclusión financiera.

ODS 9: Industria, innovación e infraestructura

La implementación de este proyecto implica innovación tecnológica y desarrollo de infraestructuras digitales. Esto podría mejorar la eficiencia de los procesos financieros y fomentar la inclusión financiera, promoviendo así el crecimiento económico sostenible.

ODS 10: Reducción de las desigualdades

Al proporcionar una identidad financiera digital a través de *Blockchain*, se podrían reducir las desigualdades al permitir un acceso más equitativo a los servicios financieros (Thomason, 2021). Esto daría a las personas en situaciones desfavorecidas la oportunidad de participar más activamente en la economía y mejorar sus condiciones de vida.

ODS 12: Producción y consumo responsables

La adopción de *Proof of Stake* (*PoS*) en la *Blockchain* de *Ethereum* en 2022, en lugar del sistema de consenso *Proof of Work* (*PoW*), ha tenido un impacto positivo en la eficiencia energética de la plataforma (Tyagi, Goyal, & Kumar, 2022). *PoS* consume significativamente menos energía en comparación con *PoW*, lo que contribuye a reducir la huella ecológica de las aplicaciones basadas en *Ethereum* y promover prácticas más sostenibles en el procesamiento de transacciones.

Por otro lado, al minimizar el número de operaciones necesarias en el *Smart Contract*, el proyecto puede reducir el consumo de recursos y la carga ambiental asociada. Al diseñar los contratos de manera eficiente, se optimiza el uso de recursos computacionales y se reduce el impacto ecológico de la ejecución de transacciones en la *Blockchain*.

ODS 16: Paz, justicia e instituciones sólidas

El uso de *Blockchain* puede contribuir a la transparencia y la integridad en las transacciones financieras y en las verificaciones de identidades. Esto supondría mejorar la confianza en los

sistemas financieros y fortalecer las instituciones involucradas en la gestión de identidades y transacciones.

Es importante destacar que, además de estas alineaciones mencionadas, un proyecto de identidad financiera digital basada en *Blockchain* también podría contribuir a otros ODS, como la igualdad de género, la educación de calidad y la acción por el clima, dependiendo de la forma en que se promueva su impacto en la sociedad y el medio ambiente.

ANEXO II: GUÍA DE INSTALACIÓN Y FUNCIONAMIENTO PARA EL USUARIO

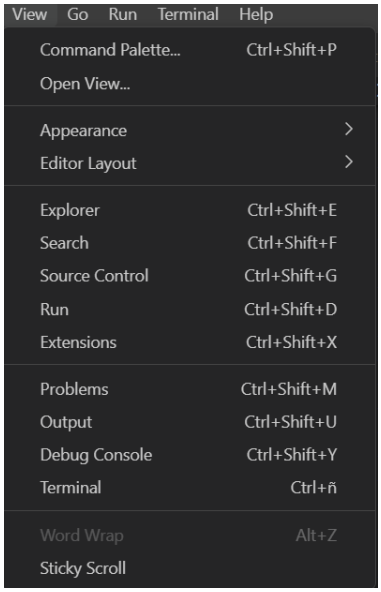
En este anexo se detallan los pasos a seguir para instalar el proyecto y utilizar la aplicación desarrollada.

El sistema operativo para el desarrollo del proyecto ha sido Windows 10 y se ha trabajado con la consola de Windows o símbolo del sistema.

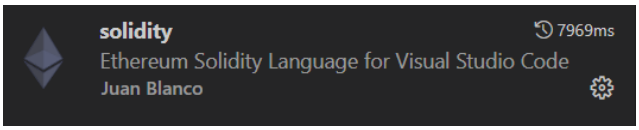
Visual Studio Code

Visual Studio Code es un editor de código gratuito que se puede descargar en el siguiente link: https://code.visualstudio.com/download

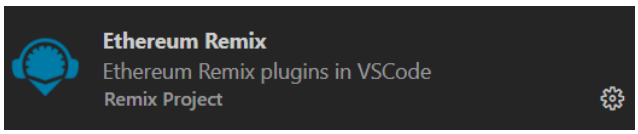
Una vez instalado, se debe instalar la extensión de *Solidity* para poder editar el código del *Smart Contract*. Para ello se usa la barra de herramientas superior, se hace clic en *View* y después en *Extensions*.



La extensión que se ha instalado es la siguiente:



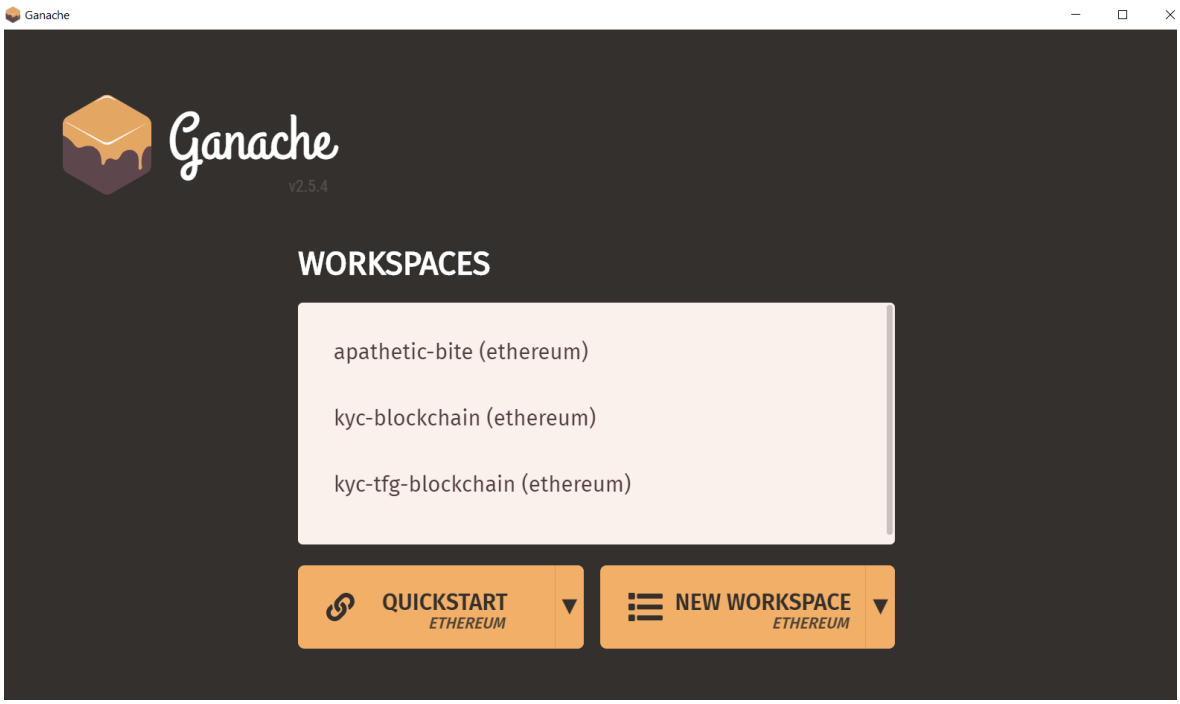
También es necesario instalar la extensión de *Remix* para poder llevar a cabo la compilación y el despliegue del *Smart Contract*.



Ganache

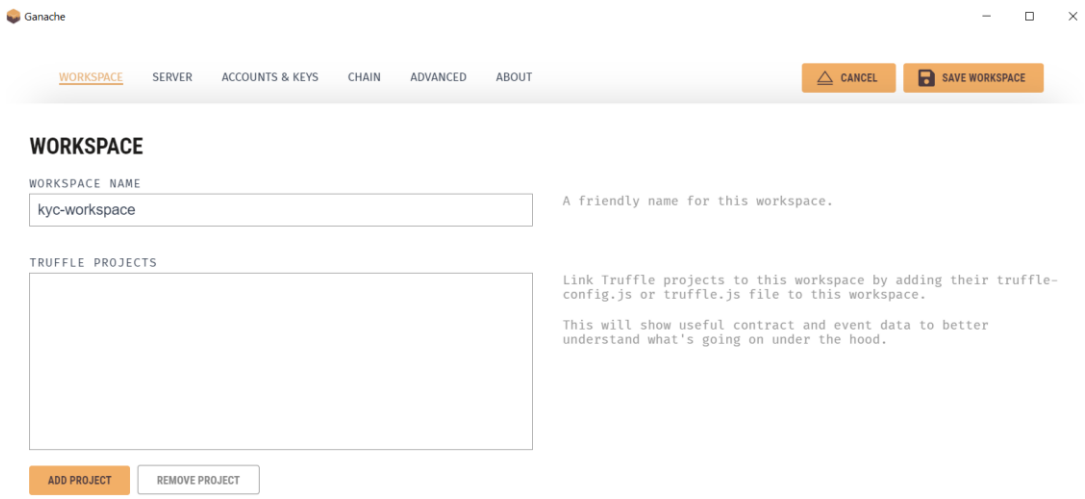
Para poder crear una red de *Ethereum* con la que simular el sistema a desarrollar, se debe instalar y usar *Ganache*. Se puede obtener en el siguiente link: https://trufflesuite.com/ganache/

Una vez instalado, se debe crear un *workspace* pulsando en *New Workspace*.

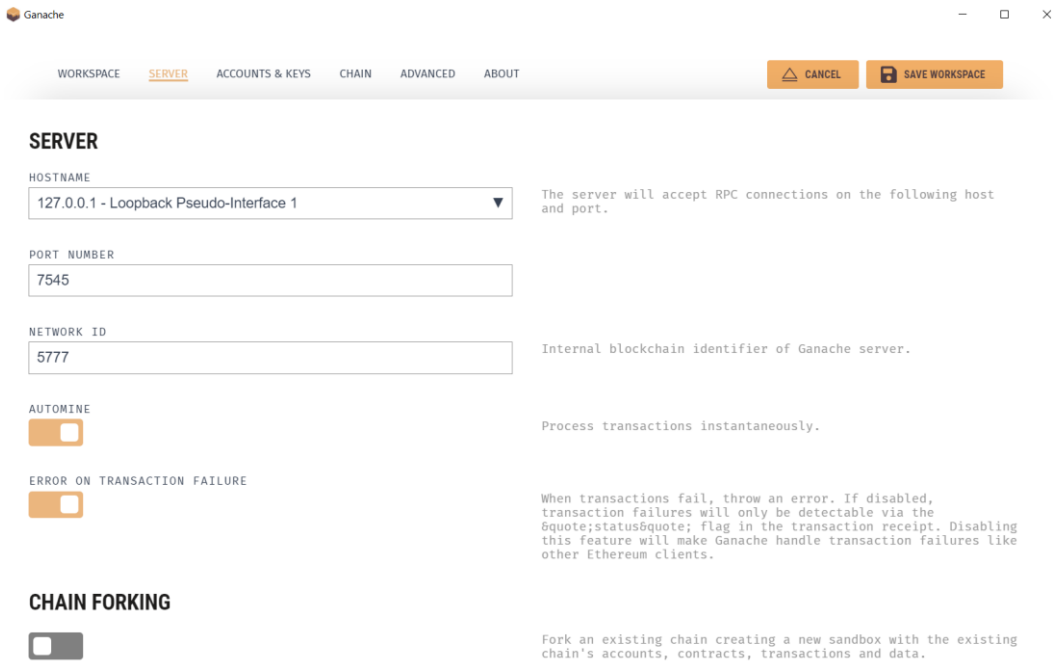


Para configurar el *workspace* e integrarlo en el proyecto se siguen los siguientes pasos:

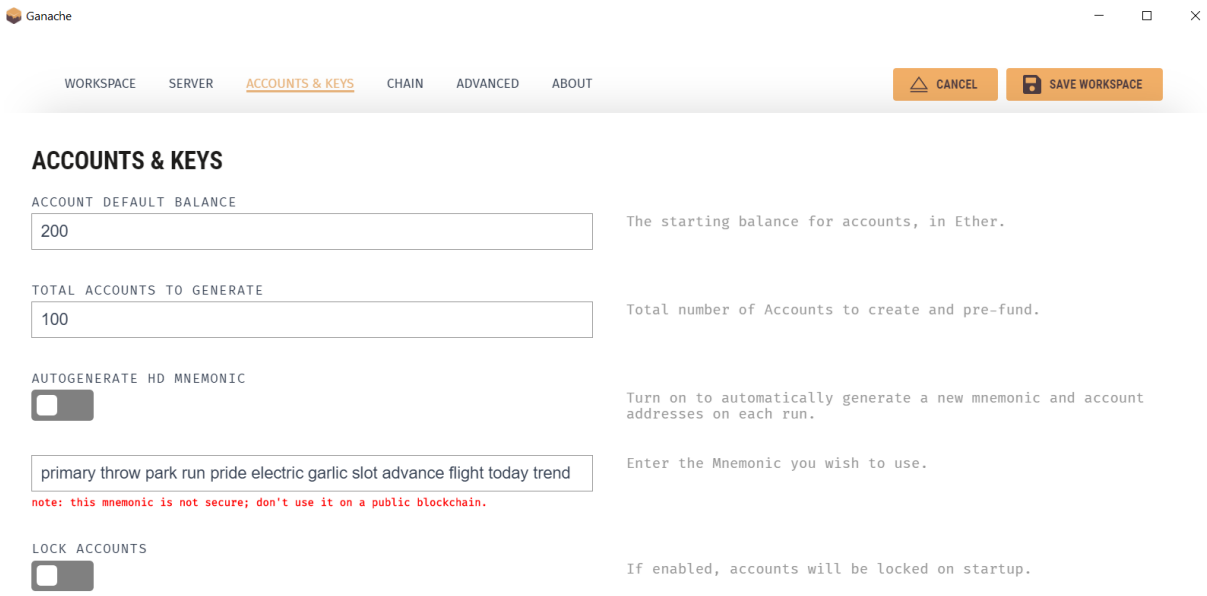
1 - En la pestaña WORKSPACE: asignar un nombre al *workspace*



2 – En la pestaña SERVER: dejar los valores por defecto (el puerto 7545 se ha usado para el proyecto, pero podría cambiarse si se cambia también en *JavaScript*).

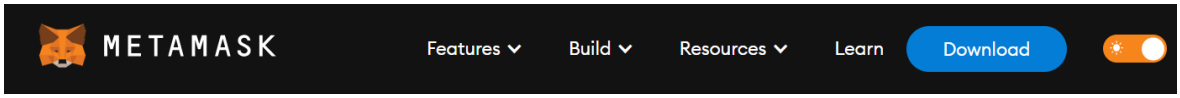


3 – En la pestaña ACCOUNTS & KEYS: crear 100 o menos cuentas y asignar 200 *ethers* a cada una.



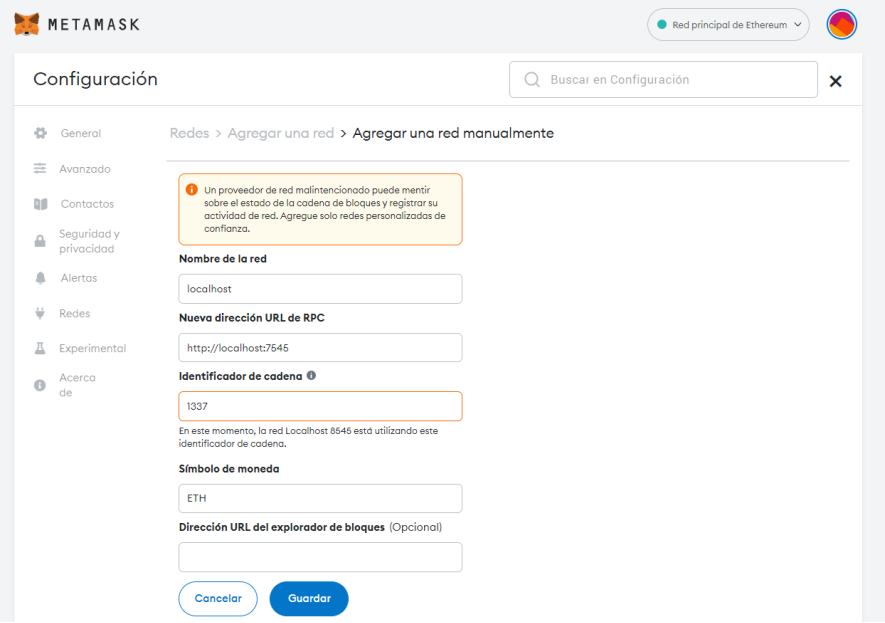
Conexión de la *wallet* de *MetaMask*

Primero se debe instalar la extensión de *MetaMask*. Se debe visitar el enlace https://metamask.io/. En la barra de menú, se pulsa descargar (*Download*).

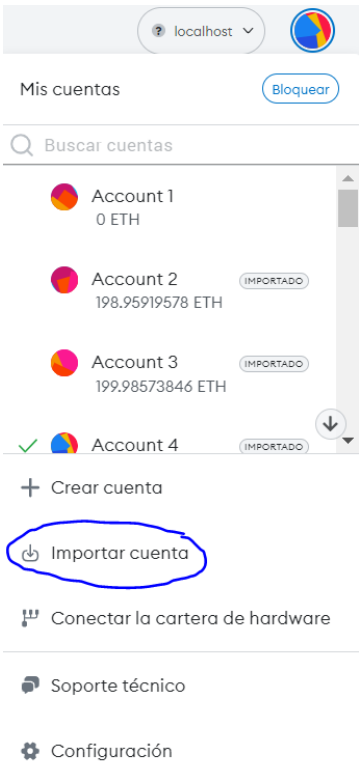


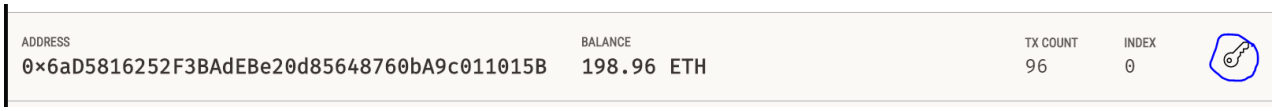
Una vez instalada, se abrirá automáticamente y permitirá crear una cuenta. *MetaMask* proporciona una frase mnemotécnica de recuperación de la clave o contraseña de 12 palabras. Es esencial guardar esta frase de forma segura.

Una vez creada la cuenta, se entra en la configuración de la extensión para añadir una red. Se añade la red *localhost* en el puerto 7545, ya que ahí es donde se ha configurado *Ganache*.



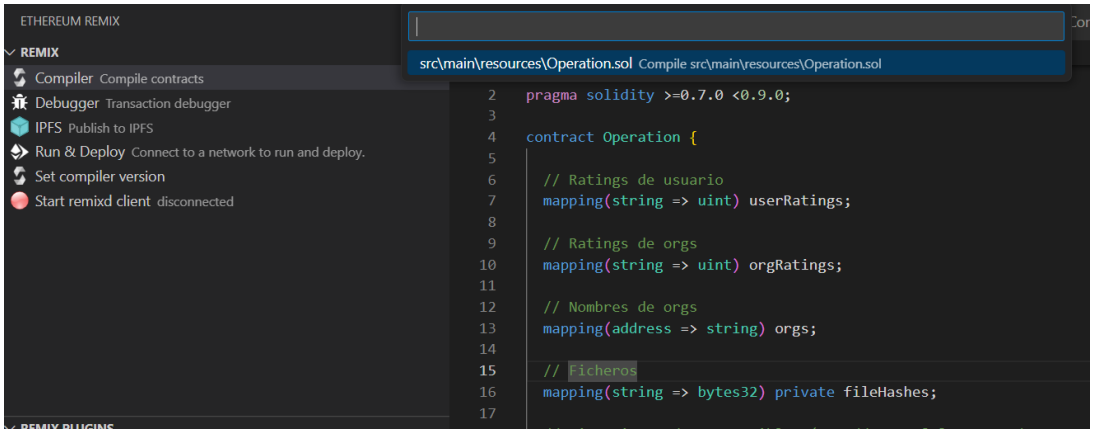
Una vez configurada la red, se importan todas las cuentas. Para ello es necesario copiar sus claves privadas de *Ganache*.

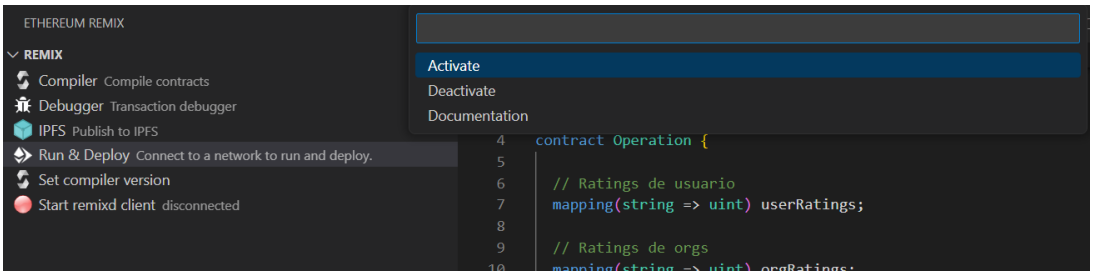




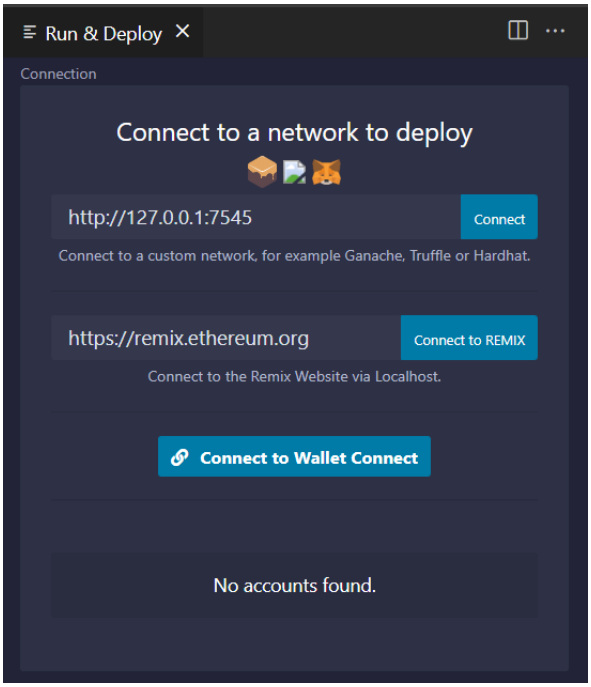
Compilación y despliegue del *Smart Contract*

Una vez guardado y abierto el *workspace* de *Ganache*, se abre la extensión *Remix* (suele tardar unos minutos) y se compila el *Smart Contract* (Operation.sol). Se conecta *Remix* a la dirección en la que se ha configurado *Ganache* previamente y se hace *Run & Deploy* del contrato, y luego *Activate*.

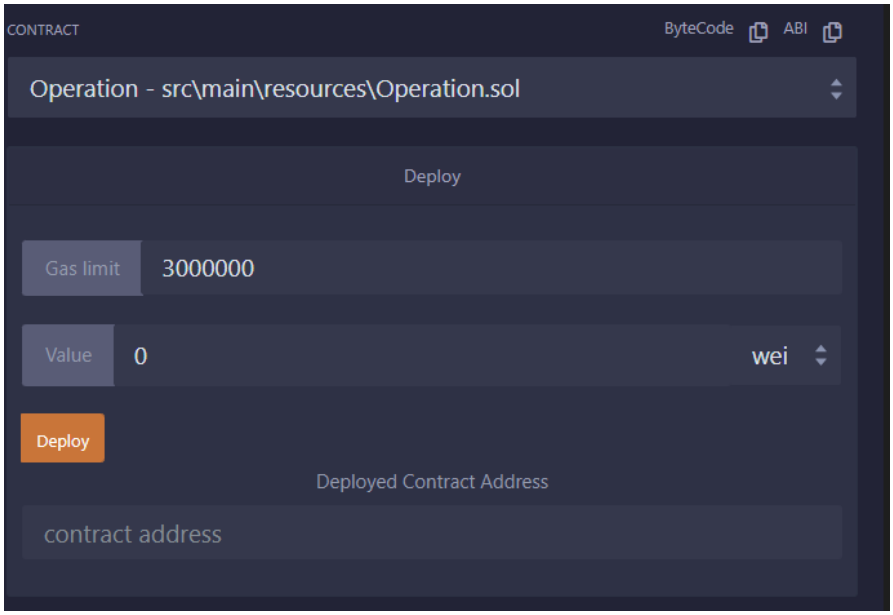




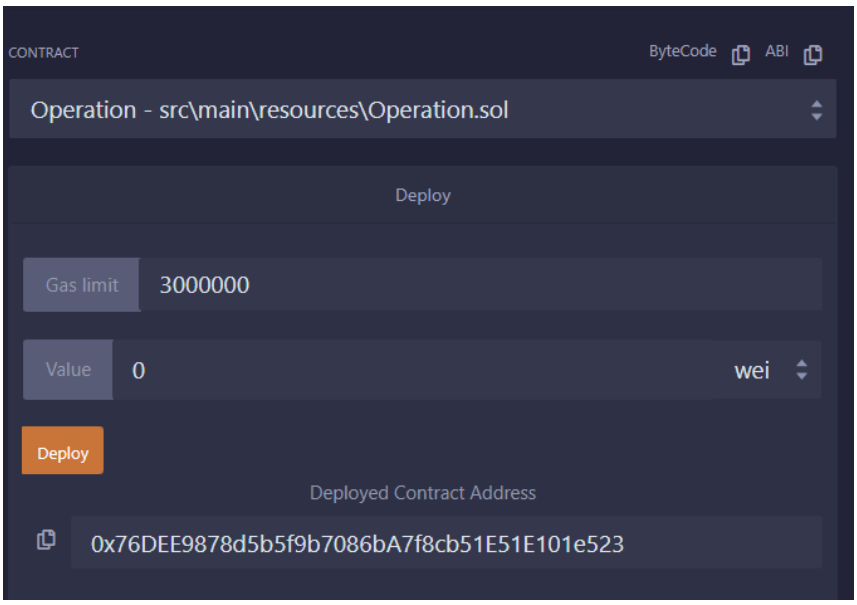
Una vez hecho el *Activate*, se abrirá una segunda ventana de *Remix* como se muestra a continuación:



Se debe conectar a la red de *Ganache* lanzada previamente, pulsando en *Connect*.



Una vez conectado, se vuelve a dar a *Deploy* en la ventana abierta de *Remix*. Se obtendrán valores de *Deployed Contract Address* y *ABI*.



Se copian los valores obtenidos de *Deployed Contract Address* y *ABI* a los siguientes ficheros:

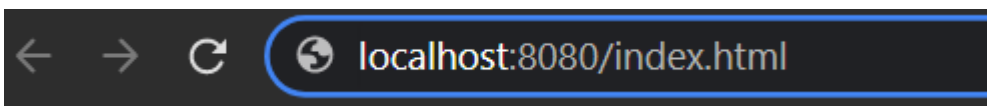
- smartcontract.js
- inicio.js

Así se asegura que las funciones que llaman al *Smart Contract* desde estos ficheros están actualizadas.

Desde la ventana de comandos de Windows, dentro de la carpeta *kyc-myid*, se ejecuta:

```
mvn spring-boot:run
```

Una vez esté en ejecución la aplicación de *Spring Boot*, se introduce la siguiente dirección en el navegador:



Así debería abrirse la página principal de la aplicación web desarrollada.

Ya estaría lista para usar y probar.

ANEXO III: MANUAL DE USUARIO

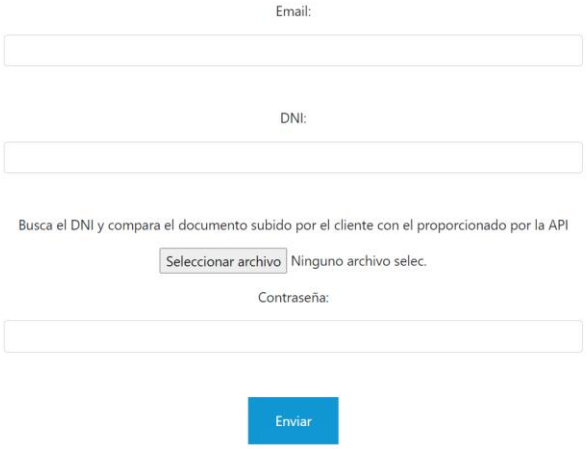
Esta sección explica cómo utilizar la interfaz gráfica del usuario, o vista del cliente, de la aplicación. Esto se lleva a cabo a través de capturas de pantalla y explicaciones breves.

PÁGINA INICIAL

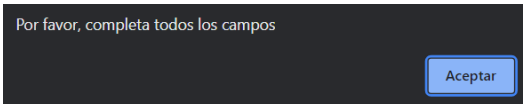
En la página inicial, el usuario puede acceder a información sobre la aplicación (*Personal*, *Empresa*, *Sobre MyID* o el botón *Más información*), iniciar sesión (*Acceso*) o registrarse (*Registro*).

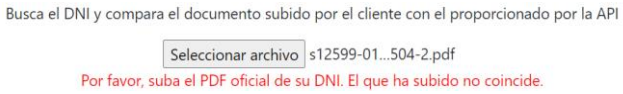
REGISTRO

La página de registro permite a los futuros usuarios u organizaciones registrarse. Para ello deben proporcionar sus datos personales y subir el PDF oficial de su DNI para que este sea verificado a través de la API del Ministerio de Interior. Si todo va bien, se registrará al nuevo usuario y se le redirigirá a la página de inicio de sesión.



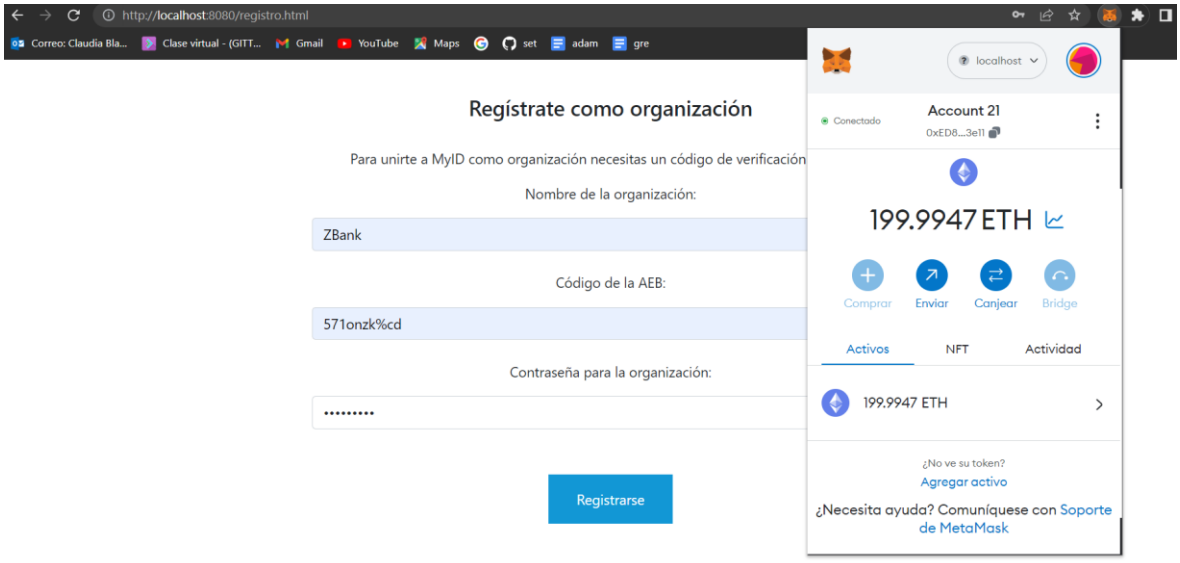
Si ocurren errores durante el registro (por ejemplo, el usuario olvida rellenar todos los campos o el PDF subido no coincide con el oficial), se comunicará al usuario el error a través de mensajes en la propia página o alertas en el navegador. Por ejemplo:





El registro de organizaciones es muy similar.

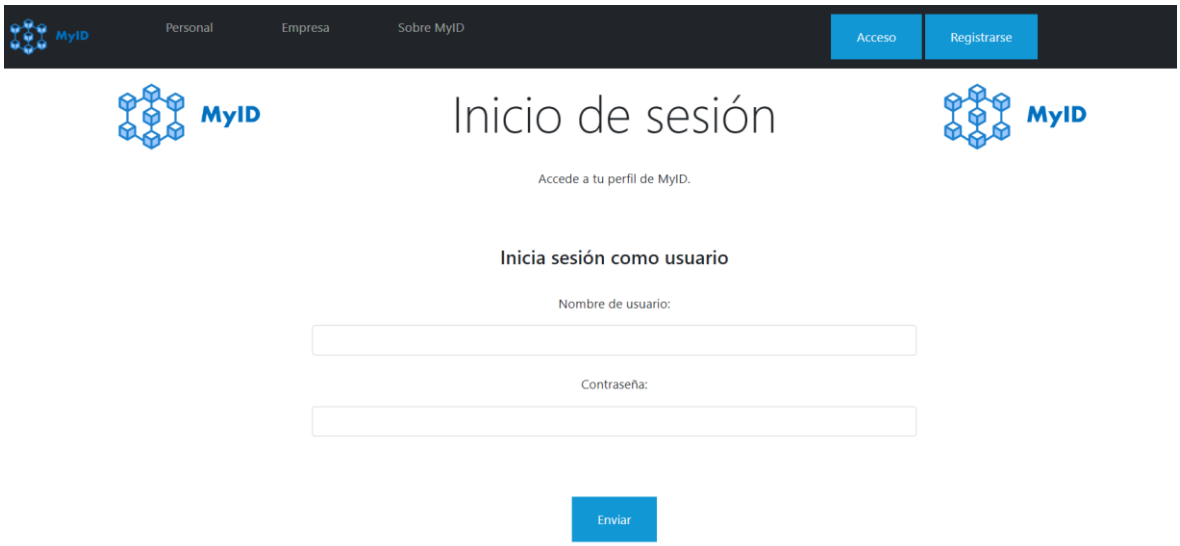
Las organizaciones deben tener una cuenta de *Ethereum* en su *wallet* de *MetaMask*. A continuación, se muestra un ejemplo de registro correcto:

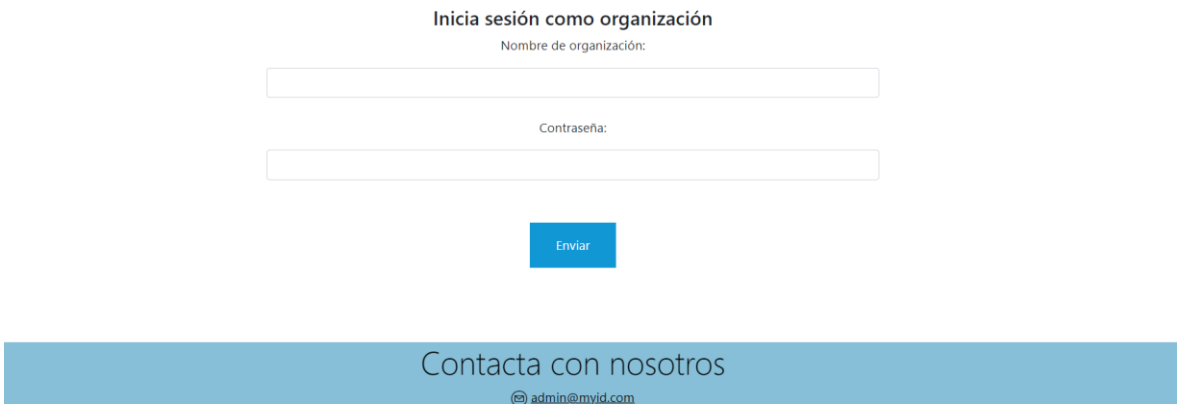


La empresa "ZBank" tiene un código otorgado por la AEB que se usa para verificar su legitimidad en el registro. Además, "ZBank" tiene conectada su cuenta (*Account 21*) a la *wallet*, y así al registrarse su nombre quedará asociado a esa dirección en la *Blockchain*.

INICIO DE SESIÓN

Los clientes pueden iniciar sesión como usuarios o como organizaciones, como se muestra a continuación.





INTERFAZ DE USUARIO

Página principal de usuario

La página inicial para el usuario una vez inicia sesión tiene el aspecto mostrado en la siguiente captura de pantalla:

Verificación de documentos con MyID

Durante tu proceso de registro en MyID, aportaste el PDF oficial tu DNI. Si lo renuevas siempre puedes actualizarlo en la sección de verificación de documentos

También tienes la opción de verificar tu declaración de la renta personales, además de una copia oficial de tu DNI en PDF, para crear una cuenta.

Ir

Más información sobre MyID

Tecnologías

MyID utiliza las tecnologías de Ethereum y MetaMask para gestionar sus verificaciones de identidad y de historiales financieros y crediticios.

Sigue el link si quieres saber más sobre MetaMask.

MetaMask

¿Qué es un proceso KYC?

KYC (Know Your Customer, o Conoce a Tu Cliente) es una práctica que llevan a cabo muchas organizaciones para verificar la identidad de sus clientes. Los procesos KYC son muy relevantes en el ámbito bancario y para entidades de crédito, pero también los llevan a cabo otros tipos de empresas, como aseguradoras o empresas de telecomunicaciones.

Qué necesitas para formar parte de MyID

Si eres una empresa o entidad bancaria, necesitar tener una cuenta en Ethereum y por tanto una address asociada.

Si quieres formar parte de MyID como usuario, necesitarás aportar algunos datos personales, además de una copia oficial de tu DNI en PDF, para crear una cuenta.

Obtener tu DNI en PDF oficial

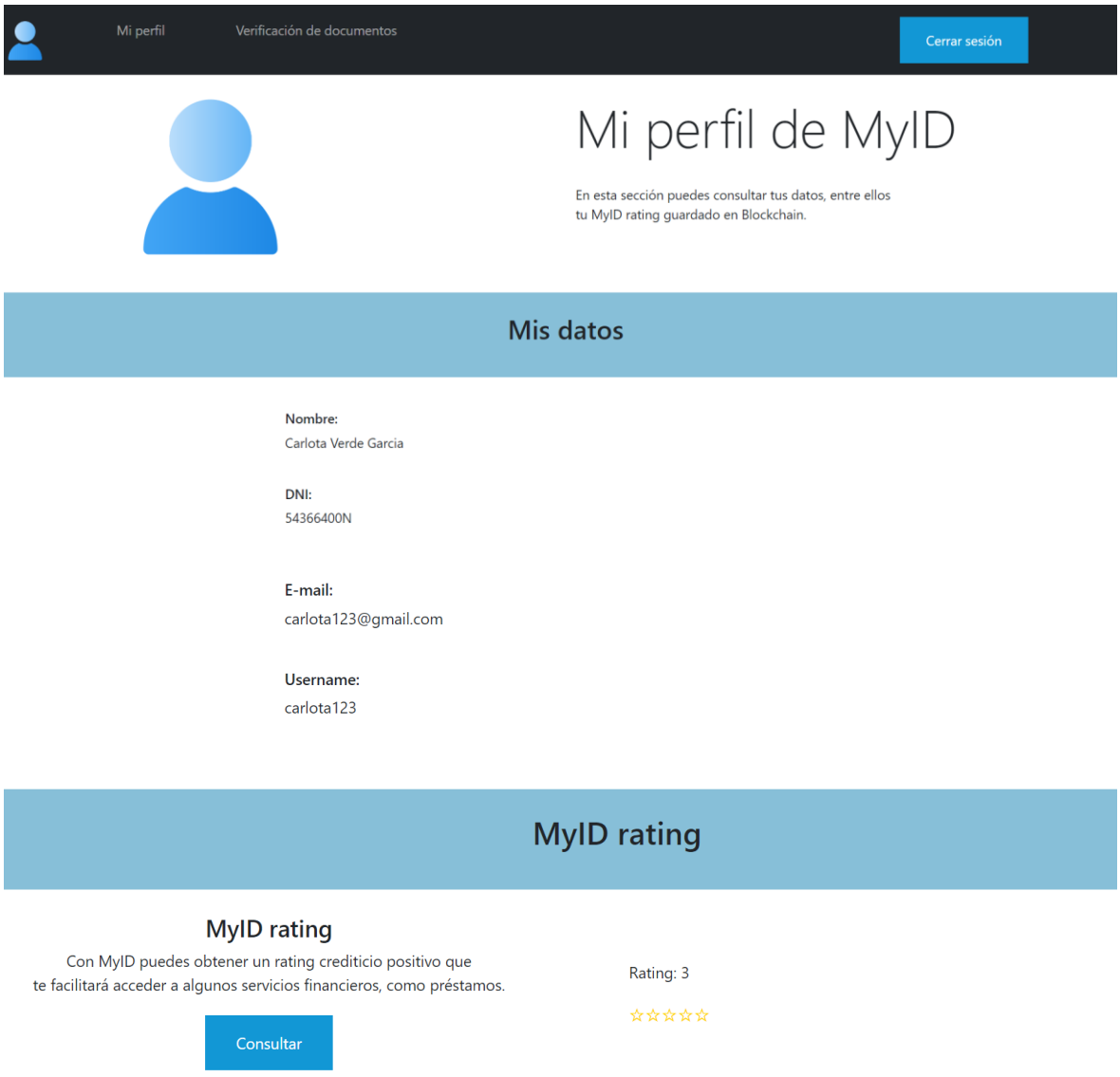
Contacta con nosotros

admin@myid.com

Como se puede observar, en la página principal tienen acceso a información sobre la aplicación y también a algunas de sus funcionalidades.

Visualización de *rating* propio para el usuario

Los usuarios pueden ver sus datos y *rating* (guardado en *Blockchain*), pulsando en *Mi perfil* en la barra de navegación o en *Saber más* sobre su MyID *rating*.



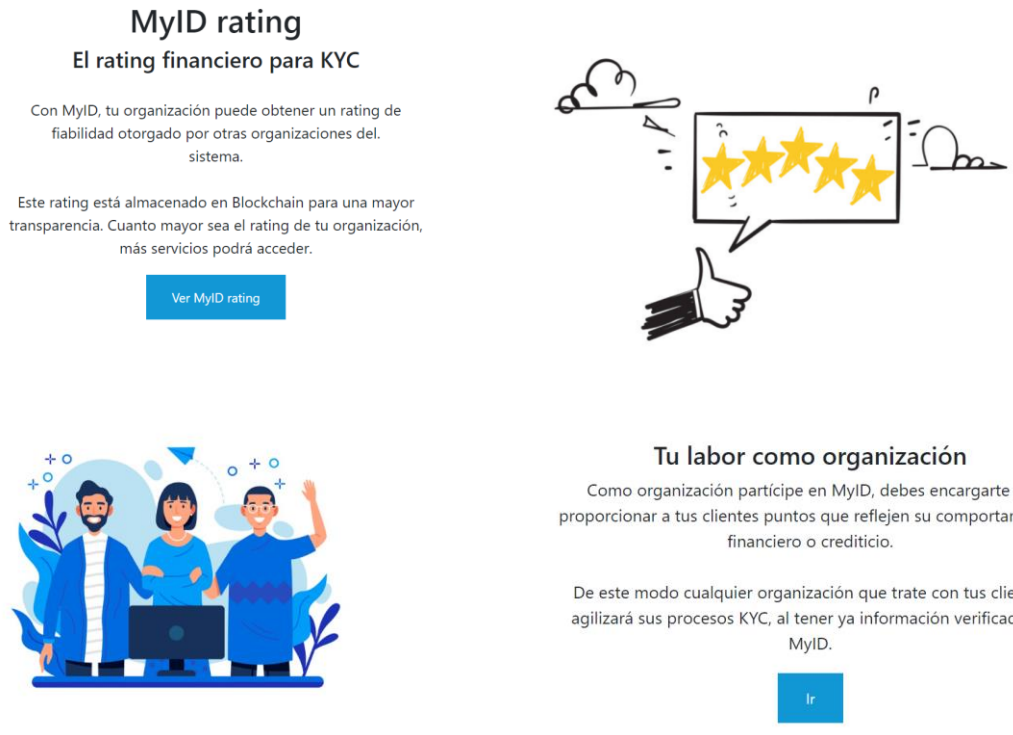
Verificación de documentos para el usuario

También pueden subir documentos. Pueden verificar su DNI de nuevo al igual que hicieron al registrarse (en caso de que, por ejemplo, lo hayan extraviado o renovado), y verificar su declaración de la renta a través de la API de Hacienda.

INTERFAZ DE ORGANIZACIÓN

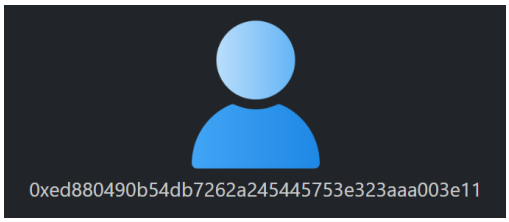
Página principal para organización

La página principal de las organizaciones, una vez inician sesión, tiene el siguiente aspecto:



Como se puede observar, es muy similar a la página principal de los usuarios, pero las organizaciones tienen acceso a funcionalidades diferentes.

Además, en la barra de navegación, bajo el icono de usuario, aparece su dirección de *Ethereum*.

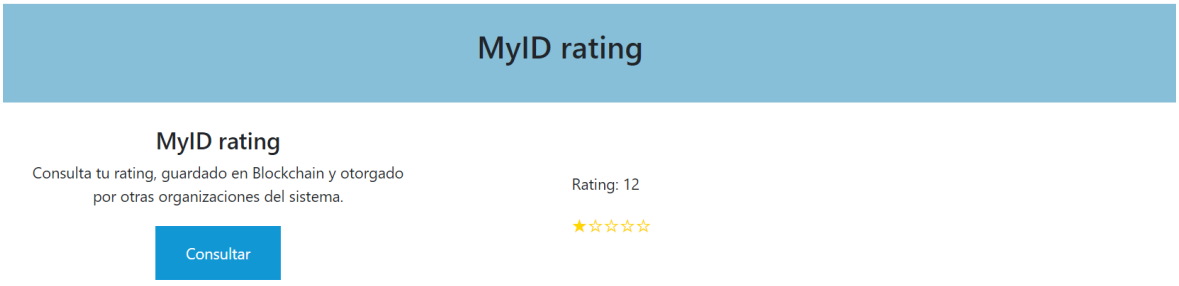


Todas las organizaciones pueden ver su propio *rating*, buscar el *rating* de una persona por DNI, dar o quitar votos a usuarios, y puntuar a otras organizaciones.

Consulta de *rating* propio para organizaciones

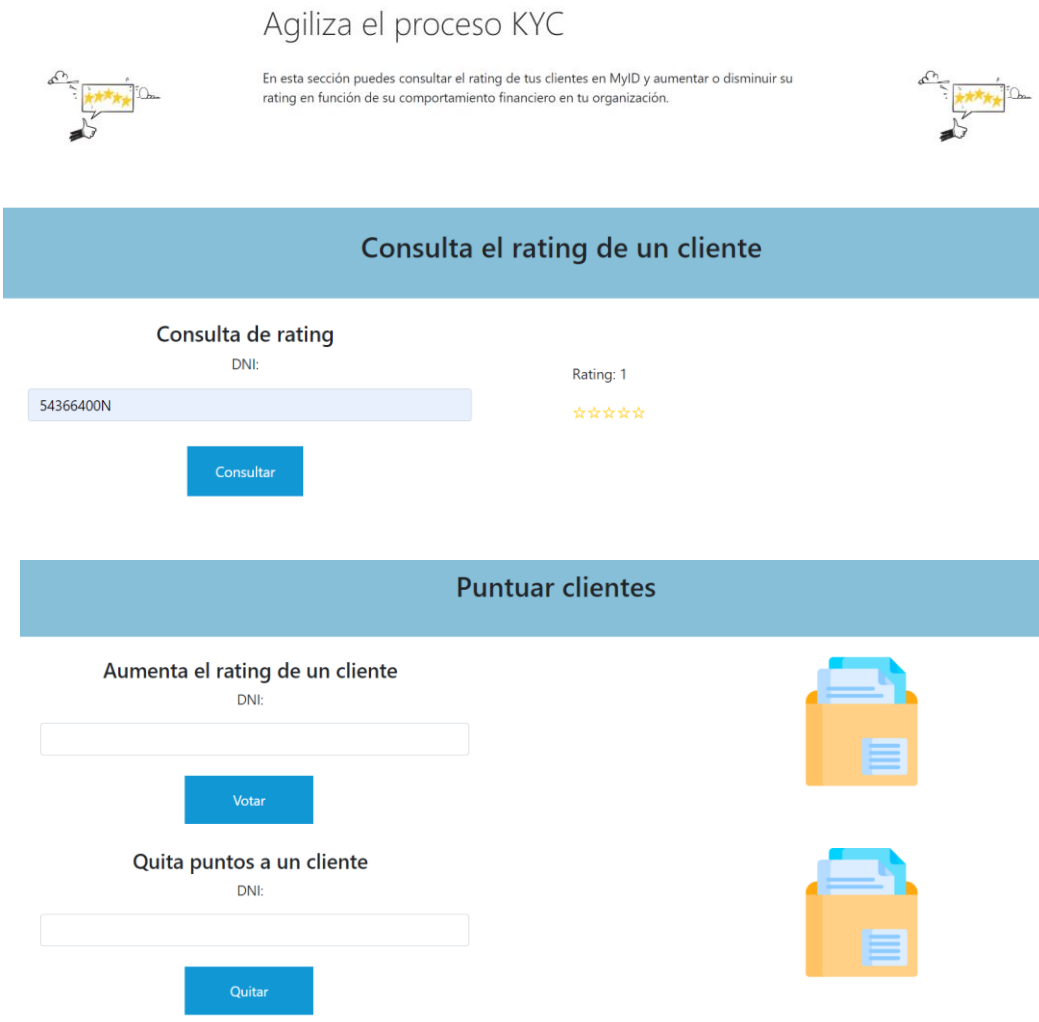
En *MyID rating* ven lo siguiente:

Las estrellas del *rating* se van modificando en proporción a su *rating*. Un *rating* de 5 no supone 5 estrellas. Un *rating* de 12, por ejemplo, implica 1 estrella.



Consulta y modificación de *rating* de clientes para organizaciones

Las organizaciones también pueden buscar el *rating* de un cliente por DNI, y otorgar o quitar puntos a los clientes, en *Rating de clientes*:

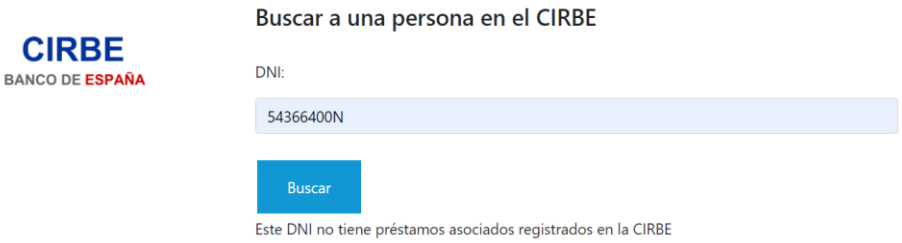


Las organizaciones con más de una cierta puntuación tienen la opción de puntuar a los clientes en 2 o 4 unidades, según el tipo de comportamiento financiero que quieran reflejar:

Verificación de documentos de clientes para organizaciones

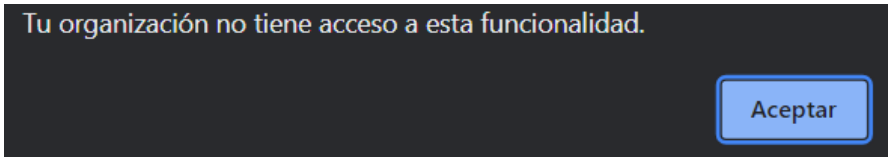
Estas organizaciones también pueden hacer "chequeos extra" utilizando las APIs del Ministerio del Interior, la Agencia Tributaria, el CIRBE y ASNEF.

En el caso del CIRBE y ASNEF, pueden buscar a usuarios por su DNI en dichas APIs. En la siguiente captura se muestra el caso en el cual el cliente no tiene ningún historial en el CIRBE:

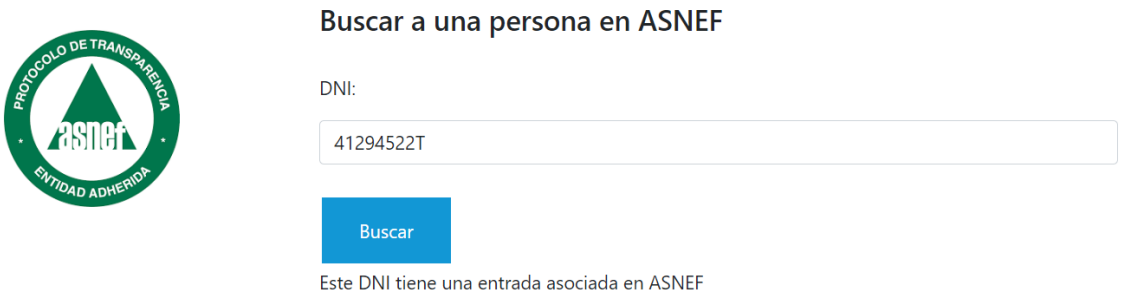


La siguiente captura muestra el caso en el cual el cliente sí tiene historial en el CIRBE:

Si una organización con una puntuación inferior a 8 intenta buscar a un usuario en la API, no se le permitirá acceder y se le mostrará un mensaje como el siguiente:



La búsqueda en ASNEF funciona de manera similar:



La verificación de documentos requiere que la organización introduzca tanto el DNI del usuario como el documento proporcionado. Se llevará a cabo una verificación en *Blockchain* y con la API externa.

Si el documento no está verificado, se informa a la organización, como se muestra a continuación:

En este caso el documento que ha subido el usuario no está verificado en la red de *Blockchain*. En este caso la organización podría informar al cliente de ello; lo más probable es que el cliente haya renovado su DNI, pero haya olvidado actualizarlo en su cuenta en la aplicación.

La verificación de la declaración de la renta es similar:

Aumento de *rating* de otras organizaciones

Las organizaciones también pueden votar a otras organizaciones, pero para ello necesitan conocer su *address* en *Ethereum*.