Implementación de la Identidad Digital con blockchain e inteligencia artificial

Frank Cespedes Ruiz

Universitat Oberta de Catalunya

Aplicaciones y Sistemas Distribuidos

Nombre Tutor/a de TF
Amadeu Albós Raya
Profesor/a responsable de la asignatura
Joan Manuel Marqués
Fecha Entrega
09/01/2024

FICHA DEL TRABAJO FINAL

Título del trabajo:	***Implementación de la Identidad Digital con blockchain e inteligencia artificial***
Nombre del autor:	*Frank Céspedes Ruiz*
Nombre del consultor/a:	*Amadeu Albós Raya*
Nombre del PRA:	*Joan Manuel Marqués*
Fecha de entrega (mm/aaaa):	*01/2024*
Titulación o programa:	*Grado de Ingeniería informática*
Área del Trabajo Final:	*Aplicaciones y sistemas distribuidos*
Idioma del trabajo:	*Catalán, castellano o inglés*
Palabras clave	*Identidad digital, Inteligencia Artificial, Blockchain*

Resumen del Trabajo

Este Trabajo de Fin de Grado aborda el problema crítico de la identidad digital en la era moderna, proporcionando una solución que integra inteligencia artificial para el reconocimiento facial y tecnología blockchain para el almacenamiento seguro y la verificación de identidad. Dada la creciente prevalencia de fraudes de identidad y brechas de datos, este sistema busca ofrecer un método de autenticación y verificación más seguro, transparente y controlable por el usuario.

La metodología utilizada se basa en el desarrollo de algoritmos de reconocimiento facial apoyados en inteligencia artificial para la identificación precisa de individuos. Estos datos son posteriormente vinculados a una blockchain híbrida, desarrollada con el framework Substrate, permitiendo la interoperabilidad a través de parachains. Este enfoque descentralizado no solo refuerza la seguridad, sino que también facilita el intercambio seguro de credenciales entre diferentes dominios y jurisdicciones.

Los resultados indican que este enfoque multidisciplinario logra ofrecer un mecanismo robusto para la gestión de la identidad digital. La solución demuestra ser no solo precisa en la identificación, sino también resistente a fraudes y en conformidad con regulaciones como el GDPR, al mantener los datos sensibles en nodos blockchain privados.

En conclusión, este trabajo pone de manifiesto cómo la confluencia de inteligencia artificial y blockchain puede ofrecer una solución viable y escalable para el manejo de identidades digitales, destacando las posibilidades de una gobernanza de identidad más segura, transparente y centrada en el usuario.

Abstract

This Final Degree Project addresses the critical problem of digital identity in the modern era, providing a solution that integrates artificial intelligence for facial recognition and blockchain technology for secure storage and identity verification. Given the increasing prevalence of identity fraud and data breaches, this system aims to offer a more secure, transparent, and user-controllable method of authentication and verification.

The methodology used is based on the development of facial recognition algorithms supported by artificial intelligence for the accurate identification of individuals. These data are subsequently linked to a hybrid blockchain, developed with the Substrate framework, allowing interoperability through parachains. This decentralized approach not only reinforces security but also facilitates the secure exchange of credentials between different domains and jurisdictions.

The results indicate that this multidisciplinary approach successfully provides a robust mechanism for managing digital identity. The solution proves to be not only accurate in identification but also resistant to fraud and in compliance with regulations such as GDPR, by keeping sensitive data in private blockchain nodes.

In conclusion, this work highlights how the confluence of artificial intelligence and blockchain can offer a viable and scalable solution for handling digital identities, underscoring the possibilities for more secure, transparent, and user-centered identity governance.

Índice

1. Introducción 1
1.1 Objetivos del Trabajo 1
1.2 Impacto en sostenibilidad, ético-social y de diversidad 2
1.3 Enfoque y método seguido 3
1.4 Planificación del Trabajo 4
1.5 Breve sumario de productos obtenidos 6
1.6 Breve descripción de los otros capítulos de la memoria 7
2. Materiales y métodos 8
2.1 Definición de identidad 8
2.2 Importancia de la identidad digital 8
2.3 Desafíos Técnicos en Métodos de Identificación Actuales 9
2.4 Resolviendo la problemática de identidad digital con Blockchain 10
2.5 Comprendiendo la identidad descentralizada 10
2.6 Navegando hacia la identidad autosoberana con Blockchain 11
2.7. Explorando casos de uso de DIDs 12
3. Reconocimiento Facial 14
3.1 Modelos pre-entrenados para el reconocimiento facial 14
3.2 FaceNet: Un modelo pre-entrenado para reconocimiento facial 16
3.2.1 Introducción a FaceNet 16
3.2.2 Arquitectura de FaceNet 18
3.2.3 Ventajas de FaceNet para la Autenticación Facial 18
3.3 Implementación 19
4. Substrate 21
4.1 Introducción a Substrate 21
4.2 Características Clave de Substrate 21
4.3 Arquitectura de Substrate 22
4.4 Implementación con Pallets 23
5. Descripción, documentación y Ejecución del proyecto 25
5.1 Estructura del proyecto 25
5.2 Configuración y preparación del entorno 25
5.2.1 Configuración del Substrate Node Template 26
5.2.2 Configuración del Substrate Front End Template 27
5.3 Despliegue y Ejecución 28
6. Conclusiones y trabajos futuros 32
6.1 Resumen de Conclusiones 32
6.2 Evaluación de Objetivos Planteados Inicialmente 32
6.3 Análisis de la Planificación y Metodología Seguida 33
6.4 Evaluación de Impactos 34
6.5 Trabajos Futuros 34
7. Glosario 36
8. Bibliografía 38

1. Introducción

En una era definida por la acelerada digitalización y la evolución constante de tecnologías emergentes, enfrentamos desafíos significativos en la seguridad y autenticación de la identidad digital. Vivimos en un mundo cada vez más interconectado, donde actividades como transacciones financieras y interacciones sociales se realizan en línea, aumentando la necesidad de métodos seguros y confiables para autenticar identidades.

Los métodos convencionales de autenticación, como contraseñas, códigos de verificación y tarjetas de identificación, han demostrado ser insuficientes ante las crecientes amenazas cibernéticas y vulnerables a ataques y filtraciones. Esto se evidencia en incidentes como la violación de datos de Microsoft en diciembre de 2019, que expuso 250 millones de registros de clientes, resaltando la urgencia de abordar estas vulnerabilidades [1].

En este contexto, donde los métodos tradicionales están perdiendo efectividad y las preocupaciones sobre la privacidad y seguridad de los datos se intensifican, se hace imperativo encontrar soluciones más seguras, escalables y éticas. La verificación de la identidad es crucial no solo para la seguridad individual, sino también para la integridad de sistemas más amplios, como redes sociales, plataformas financieras y sistemas gubernamentales.

Hasta la fecha, se han propuesto múltiples soluciones, pero estas a menudo enfrentan problemas de escalabilidad, interoperabilidad y cuestiones éticas relacionadas con la recopilación y almacenamiento de datos. En este proyecto, proponemos abordar estos desafíos mediante la integración de dos tecnologías emergentes: la biometría facial construida con inteligencia artificial y una blockchain* híbrida para el almacenamiento seguro y transparente de la identidad digital. La adopción de blockchain, un sistema distribuido y descentralizado, es fundamental en este contexto. Al distribuir los datos a través de una red de nodos, en lugar de centralizarlos en un solo punto, se aumenta significativamente la seguridad contra ataques y filtraciones. Esta descentralización no solo mejora la resistencia a intentos maliciosos, sino que también ofrece una mayor transparencia y trazabilidad de las operaciones, aspectos críticos en la gestión de identidades digitales. Además, se adoptará el concepto de parachains para permitir la interconexión de diversas blockchains, mejorando así la eficiencia y flexibilidad del sistema.

El objetivo es desarrollar un prototipo funcional que sirva como base para sistemas de identidad digital más seguros, rápidos y éticos, adaptándose fácilmente a distintos contextos y necesidades [2-5].

1.1 Objetivos del Trabajo

El propósito principal de este trabajo es explorar y analizar las tecnologías emergentes de reconocimiento facial y blockchain para desarrollar un sistema de autenticación y proveedor de identidades robusto y descentralizado. La integración de estas tecnologías puede ofrecer mejoras significativas en la eficiencia de procesamiento de datos y en la protección de los mismos. A

continuación, se detallan de manera más precisa los objetivos específicos del proyecto.

Objetivo 01: Estudio de blockchain y modelos aplicables
Investigar cómo funciona la tecnología blockchain y determinar los modelos más apropiados para adaptarlos a la plataforma propuesta. Se debe considerar el papel de blockchain en la gestión y verificación de la identidad digital y se debe realizar una revisión de proyectos existentes que han utilizado la tecnología blockchain para abordar desafíos en el ámbito de la identidad digital.

Objetivo 02: Estudio de la inteligencia artificial y modelos pre-entrenados
Explorar en profundidad la inteligencia artificial, centrándose en los modelos pre-entrenados como herramientas clave en el desarrollo del sistema. Este objetivo implica entender cómo estos modelos pueden ser integrados y utilizados eficazmente en el sistema propuesto. Analizar cómo la IA potencia el reconocimiento facial y explorar su aplicación en sistemas de autenticación y verificación de identidad

Objetivo 03: Análisis de proyectos con ambas tecnologías
Examinar proyectos que han integrado IA y blockchain, destacando cómo cada tecnología contribuye al proyecto y sus posibles limitaciones. Es importante entender que blockchain puede hacer que la IA sea más coherente y comprensible, facilitando la trazabilidad total de los procesos de toma de decisiones.

Objetivo 04: Profundizar en como combinar ambas tecnologias
Profundizar en cómo se puede explotar al máximo las capacidades de blockchain e IA. Esto incluye comprender el uso de algoritmos hash, firmas digitales y zero-knowledge proofs para compartir y autenticar datos digitales sin revelar información sensible.

Además de los objetivos mencionados, una vez desarrollado y desplegado el sistema, se llevará a cabo una evaluación para determinar su eficacia, seguridad y eficiencia en diferentes escenarios y condiciones. Este análisis incluirá pruebas de rendimiento y seguridad en condiciones reales o simuladas. Los resultados obtenidos serán fundamentales para identificar las limitaciones del sistema y sugerir futuras líneas de mejora y desarrollo, con el fin de llevar el sistema a un nivel de madurez superior y explorar su interoperabilidad con otras tecnologías y sistemas.

1.2 Impacto en sostenibilidad, ético-social y de diversidad

Sostenibilidad

- **Positivo:**
  - **ODS 7 (Affordable and clean energy)**: Reducción en el consumo de energía.
  - **ODS 12 (Responsible consumption and production):** Menor generación de residuos electrónicos.
  - **ODS 13 (Climate action)**: Disminución del consumo de energía, contribuyendo a la lucha contra el cambio climático.
- **Negativo:**

- **ODS 7 (Affordable and clean energy)**: Desafíos en el mantenimiento de una energía sostenible.
- **ODS 13 (Climate action):** Posible impacto negativo en la lucha contra el cambio climático.

Ético-Social

- **Positivo:**
  - **ODS 16 (Peace, justice and strong institutions)**: La descentralización de datos y el control del usuario sobre su propia información supone un avance ético, ya que respeta la privacidad y la autonomía del individuo
- **Negativo:**
  - **ODS 16 (Peace, justice and strong institutions)**: El reconocimiento facial, si se implementa incorrectamente, podría dar lugar a problemas éticos como el sesgo racial o de género en la autenticación

Diversidad y Derechos Humanos

- **Positivo:**
  - **ODS 5 (Gender equality)**: Promoción de sistemas seguros y accesibles para todos.
  - **ODS 10 (Reduced inequalities)**: Apoyo a sistemas más inclusivos y equitativos.
- **Negativo:**
  - **ODS 10 (Reduced inequalities)**: Si el sistema no se diseña teniendo en cuenta la diversidad, podría ser menos efectivo o incluso discriminatorio para ciertos grupos.

1.3 Enfoque y método seguido

Para la ejecución de este proyecto, es esencial definir tanto la estrategia como la metodología a seguir que permita un desarrollo eficiente y alineado con los objetivos planteados.

Estrategia Seleccionada: Desarrollar un Producto desde Cero

Tras evaluar las diferentes estrategias, se ha optado por "Desarrollar un Producto desde Cero" por las siguientes razones:

- **Control Completo**: Al construir un nuevo sistema desde el inicio, se obtiene un control total sobre todas las características y funcionalidades, permitiendo un diseño y una implementación más cohesivos.
- **Personalización**: Esta estrategia permite adaptar el sistema exactamente a las necesidades y especificaciones requeridas, sin las limitaciones inherentes a las plataformas existentes.
- **Innovación**: Dado el rápido desarrollo en el campo de la inteligencia artificial y blockchain, crear un nuevo producto brinda la oportunidad de incorporar nuevas ideas y tecnologías al sistema.
- **Aprendizaje Profundo:** El desarrollo desde cero exige una comprensión profunda de cada componente del sistema, lo cual es beneficioso desde un punto de vista educativo y profesional.
- **Cumplimiento Normativo:** Tener control total sobre el sistema facilita asegurar el cumplimiento de todas las leyes y regulaciones pertinentes desde el inicio.

Aunque esta estrategia puede demandar más esfuerzo y tiempo, se considera la más adecuada para alcanzar los objetivos específicos de este trabajo.

Metodología: Agile
Con la estrategia claramente definida, se adoptará la metodología Agile para el desarrollo del software. Esta metodología es especialmente apropiada para proyectos de desarrollo complejos y dinámicos, permitiendo entregas periódicas de código ya testeado, y obteniendo versiones funcionales de la aplicación que irán incorporando nuevas características y mejoras con cada entrega.
La metodología Agile se organizará de la siguiente manera:

- **Bloques**: El proyecto se dividirá en bloques de trabajo, cada uno con un conjunto de características y funcionalidades a desarrollar.
- **Iteraciones**: Cada bloque se descompondrá en iteraciones, que son ciclos de desarrollo donde se planifica, diseña, implementa y testea un conjunto de características.
- **Sprints**: Las iteraciones se ejecutarán en sprints, períodos de tiempo definidos durante los cuales se completa un conjunto específico de tareas.

Esta estructura permitirá una planificación y ejecución del trabajo de manera ordenada y eficiente, facilitando el seguimiento del progreso y la adaptación a cambios o nuevas necesidades que puedan surgir durante el desarrollo del proyecto.

1.4 Planificación del Trabajo

A continuación, se describen las principales tareas a realizar en el desarrollo del proyecto:

1. **Realización del plan de trabajo (10 dias):** Para cumplir este hito, se realiza una propuesta del tema en el que se trabajará y un análisis superficial del sistema para validarse. Tras finalizarlo, se obtiene un documento que contiene la descripción a alto nivel del trabajo a realizar, los objetivos generales y específicos del proyecto, y el plan de trabajo a seguir.
2. **Análisis de las tecnologías de Inteligencia Artificial (IA) aplicada al reconocimiento facial (10 días):** Se realizará un análisis en profundidad explorando las iniciativas y estructuras o sistemas existentes en inteligencia artificial y reconocimiento facial.
3. **Análisis de tecnologías blockchain y otras alternativas (10 días):** Se realizará un análisis de las tecnologías desarrolladas, desplegadas y conectadas con substrate y cuales se ajusten a la solución buscada.
4. **Análisis de requisitos de la solución a desarrollar (10 días):** Siguiendo el trabajo realizado hasta este punto, se realizará un análisis de requisitos funcionales y no funcionales de la solución a desarrollar. Además, se definirán los algoritmos de reconocimiento facial que se utilizarán.
5. **Diseño técnico y funcional del sistema (10 días):** Con los requisitos obtenidos, y para finalizar esta etapa de análisis y diseño, se realizará un diseño técnico y funcional del sistema a desarrollar, que incluirá la arquitectura a construir, los modelos de IA a implementar y esquemas de la blockchain a utilizar.
6. **Desarrollo del modelo de IA y la blockchain (10 días):** Se desarrollará el modelo de IA siguiendo el esquema obtenido en la tarea anterior y

utilizando el lenguaje necesario, así como la implementación de la blockchain en Substrate.

7. **Desarrollo de la interfaz de usuario y la integración del sistema (10 días):** Para completar este hito, se desarrollará la interfaz de usuario y se integrarán los componentes desarrollados en los hitos anteriores, de manera que permitan realizar las operaciones necesarias en el sistema diseñado.
8. **Testing, validación y despliegue en un entorno controlado (5 días):** Una vez la implementación ha finalizado en el entorno local, se pasarán a realizar los tests funcionales finales y a validar la solución trabajada según los distintos casos de uso definidos. Seguidamente, se desplegará en un entorno controlado para pruebas preliminares y ajustes necesarios.
9. **Conclusiones y próximos pasos (3 días):** Con el trabajo de validación realizado, se obtendrán las conclusiones finales del proyecto realizado y se establecerán los próximos pasos a dar en caso de seguir con la investigación.
10. **Finalización de la memoria y preparación de la presentación (2 días):** Esta última tarea culmina con la concentración del trabajo realizado en una memoria final del proyecto y la presentación de la investigación realizada.

Finalmente, se muestra un diagrama tentativo de la ejecución de los trabajos definidos y la consecución de los principales hitos de este TFG:

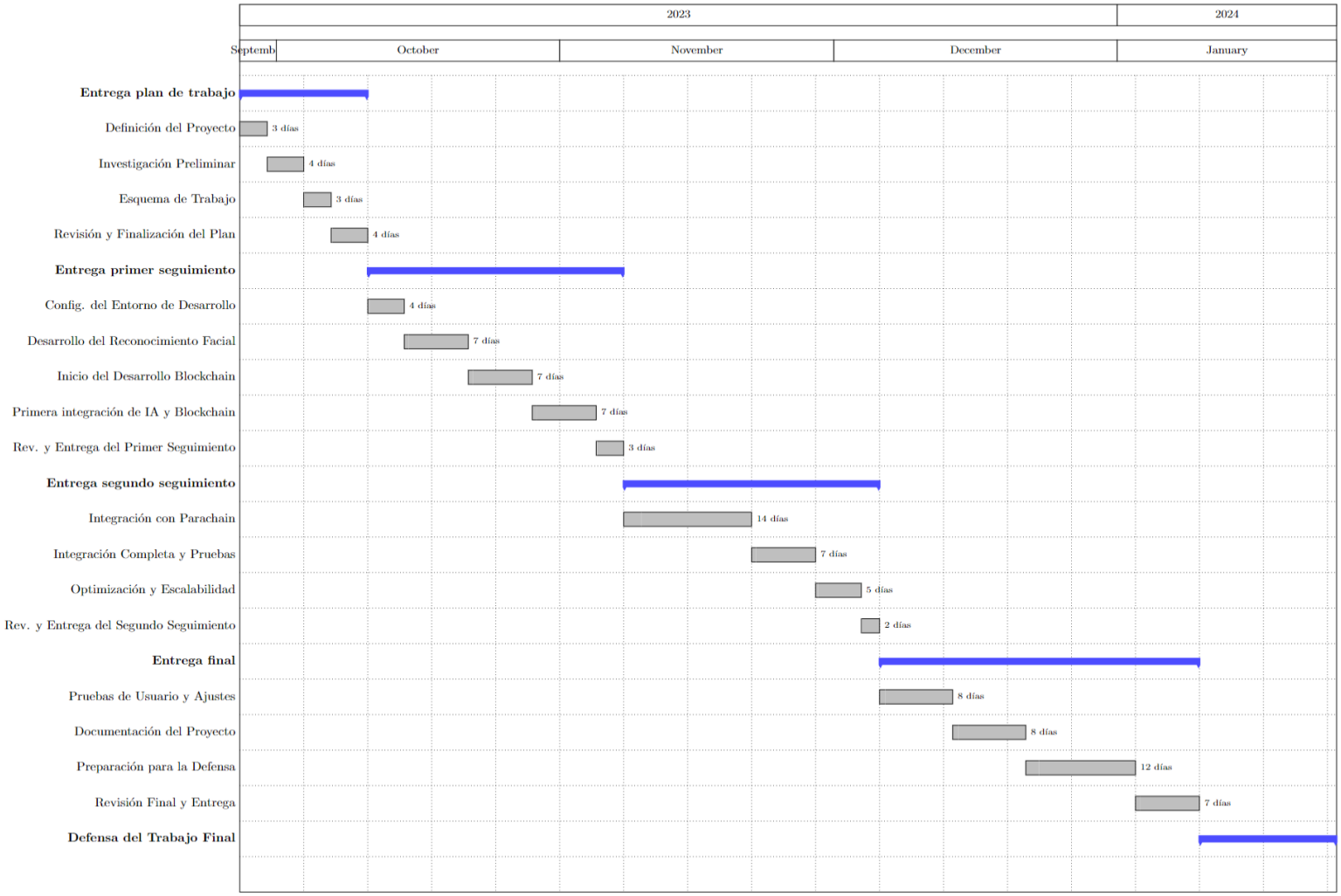


Diagrama de Gantt

1.5 Breve sumario de productos obtenidos

En este proyecto se desarrollarán dos productos principales: el "Diseño" y la "Prueba de Concepto". Cada uno de estos productos está compuesto por varias partes esenciales, que se detallan a continuación:

Producto 1: Diseño
Este producto incluye:

- **Arquitectura del Sistema**: Diseño detallado de la arquitectura del sistema, integrando reconocimiento facial basado en IA y blockchain para la gestión de la identidad digital.
- **Modelo de Reconocimiento Facial**: Diseño de un modelo de inteligencia artificial para un reconocimiento facial preciso, que forma parte del sistema de autenticación segura.
- **Blockchain Personalizada**: Diseño de una blockchain optimizada utilizando Substrate, enfocada en la gestión de datos sensibles y la autenticación.
- **Smart Contracts**: Diseño de contratos inteligentes para definir políticas de acceso y facilitar la interoperabilidad entre sistemas.
- **Interfaz de Usuario**: Diseño de una interfaz, ya sea gráfica o de línea de comandos, para la interacción y administración del sistema.

Producto 2: Prueba de Concepto
Este producto comprende:

- **Prototipo Funcional**: Desarrollo y validación de un prototipo que integra tanto el reconocimiento facial como la blockchain.
- **Pruebas y Resultados**: Realización de pruebas para validar el sistema, incluyendo resultados y métricas, alineados con la literatura sobre autenticación basada en blockchain.
- **Código Fuente**: Todo el código desarrollado para la prueba de concepto, abarcando el modelo de reconocimiento facial, blockchain, contratos inteligentes y la interfaz de usuario.

Además, por otro lado añadiremos:
Documentación:

- **Documentación Técnica**: Manuales y documentación que explican el diseño, la implementación y el uso del sistema.
- **Memoria del Proyecto:** Documento final que recoge todo el desarrollo del proyecto, desde la investigación inicial hasta la implementación y pruebas finales.

Estos productos conformarán el cuerpo principal del trabajo final, demostrando la viabilidad y eficacia de combinar inteligencia artificial con tecnología blockchain para la autenticación y autorización en cualquier entorno, facilitando la gestión auditable, rastreable y verificable de la identidad digital.

1.6 Breve descripción de los otros capítulos de la memoria

Este documento está estructurado en varios capítulos que abarcan distintas facetas del proyecto. A continuación, se describe brevemente el contenido de cada uno:

1. **Introducción**: Este capítulo sienta las bases del proyecto, describiendo el contexto, justificación, objetivos y métodos empleados.
2. **Materiales y Métodos**: Explora la definición de identidad, la importancia de la identidad digital, desafíos técnicos en métodos de identificación actuales, soluciones con blockchain, comprensión de identidad descentralizada, identidad autosoberana con blockchain y casos de uso de DIDs.
3. **Reconocimiento Facial**: Detalla modelos pre-entrenados para reconocimiento facial, en particular FaceNet, incluyendo su introducción, arquitectura, ventajas para la autenticación facial e implementación.
4. **Substrate:** Aborda la introducción a Substrate, sus características clave, arquitectura y implementación con pallets.
5. **Descripción, Documentación y Ejecución del Proyecto:** Incluye la estructura del proyecto, configuración y preparación del entorno, con detalles específicos sobre la configuración del Substrate Node y Front End Template, y el despliegue y ejecución.
6. **Conclusiones y Trabajos Futuros:** Presenta un resumen de conclusiones, evaluación de objetivos iniciales, análisis de planificación y metodología, evaluación de impactos y propuestas de trabajos futuros.
7. **Bibliografía**: Todas las fuentes académicas, artículos, y otros recursos citados en el documento.
8. **Anexos**: Este apartado contendrá todo el material adicional que apoye el proyecto, como código fuente, diagramas más detallados, o resultados de pruebas adicionales.

Cada capítulo contribuye al proyecto global, complementando y expandiendo la información que permitirá una comprensión completa del trabajo realizado.

2. Materiales y métodos

2.1 Definición de identidad

La identidad es un conjunto de características y atributos que distinguen a un individuo o entidad de otros. Este concepto, profundamente explorado en disciplinas como la psicología, la sociología y la filosofía, incluye aspectos esenciales como el nombre, edad, género, nacionalidad y atributos físicos o socioculturales. En las sociedades modernas, la identidad es un pilar clave para la identificación precisa de los ciudadanos y el funcionamiento eficaz de cualquier país [6][7][8].

Los gobiernos emplean una variedad de documentos identificativos, como el Documento de Identidad, el pasaporte y la licencia de conducir, para verificar la identidad de los individuos y facilitar procesos y transacciones. Estos documentos, que contienen datos personales clave y a menudo incorporan tecnologías avanzadas, son vitales para la autenticación de la identidad [9][10].

En paralelo, el sector del comercio electrónico enfrenta el reto de verificar la identidad de sus usuarios para garantizar transacciones seguras. El registro en plataformas online implica la solicitud de datos básicos y en ocasiones la verificación de documentos identificativos, asegurando un registro único por usuario y facilitando las transacciones.

Así, la gestión de identidades se convierte en un eje central que une a individuos, gobiernos e instituciones, así como a los comercios electrónicos, donde la evolución tecnológica está abriendo paso a soluciones de identidad digital, emergiendo como alternativas o complementos a los documentos físicos [11].

2.2 Importancia de la identidad digital

En el contexto global actual, la identificación precisa y accesible de los individuos es fundamental para el acceso a servicios básicos y la integración social. La identidad digital, emergiendo como una solución innovadora, aborda problemas clave de los sistemas de identificación tradicionales y transforma la manera en que interactuamos en el mundo digital y físico. [12]

Problemas existentes

- **Acceso a servicios esenciales:** Sin una identificación adecuada, las personas a menudo se ven impedidas de aprovechar oportunidades en educación, servicios financieros y atención médica. Esto afecta de manera significativa a poblaciones desplazadas y refugiados. La identidad digital ofrece una forma de identificación verificable y accesible para todos.
- **Transición hacia lo digital:** La gestión de identidad basada en papel es ineficiente, propensa a errores y fraudes. La identidad digital elimina estos problemas, agilizando procesos y reduciendo costos.
- **Cooperación global:** La falta de un sistema de identificación uniforme y global genera fricciones en el comercio internacional y la movilidad. Una plataforma de identidad digital estandarizada podría facilitar una cooperación internacional más fluida y segura.

Frente a estos desafíos, la identidad digital puede garantizar el acceso universal a servicios esenciales, ofreciendo una forma de identificación verificable y accesible sin depender de documentos físicos. Además, promueve una gestión de identidad más eficiente y segura, con un impacto positivo en diversos sectores como el comercio electrónico y los servicios gubernamentales.
Sin embargo, es crucial que la transición a la identidad digital se lleve a cabo con atención a la protección de la privacidad personal y la seguridad de los datos. Las políticas y tecnologías deben diseñarse para defender los derechos individuales, asegurando que la identidad digital sea no solo universalmente accesible y confiable, sino también respetuosa con la autonomía y la dignidad de cada persona.

2.3 Desafíos Técnicos en Métodos de Identificación Actuales

Los métodos actuales de identificación y autenticación enfrentan desafíos técnicos significativos, lo que subraya la necesidad de soluciones más avanzadas, como el uso de la tecnología blockchain. A continuación, se detallan los desafíos actuales, junto con cómo la transición a la blockchain podría abordarlos [12][13][14]:

1. **Vulnerabilidades de las Contraseñas:** Las contraseñas son a menudo el eslabón más débil en la seguridad. Son susceptibles a robos, filtraciones y ataques de fuerza bruta. **Blockchain** ofrece una alternativa más segura mediante el uso de claves criptográficas y autenticación multifactor basada en blockchain.
2. **Limitaciones de Tarjetas Identificativas Físicas:** Las tarjetas físicas pueden ser falsificadas o robadas. La **blockchain** permite reemplazar estas tarjetas por identidades digitales seguras, inmutables y verificables.
3. **Control Fragmentado de la Información Personal:** En los sistemas actuales, los usuarios a menudo pierden el control sobre su información personal. La identidad descentralizada en **blockchain** devuelve el control al usuario, permitiendo gestionar quién accede a su información y cómo se utiliza.
4. **Inconsistencia en Registros de Identidad:** La unificación de registros en sistemas centralizados es propensa a errores y inconsistencias. La blockchain ofrece un registro inmutable y consistente, eliminando duplicidades y errores.
5. **Multiplicidad de Puntos de Acceso Vulnerables:** Los sistemas tradicionales tienen múltiples puntos de acceso que pueden ser explotados incluyendo la centralización de los sistemas. Blockchain reduce estos puntos de acceso, proporcionando una capa adicional de seguridad a través de su estructura descentralizada.
6. **Dependencia de Terceros para la Gestión de Información Personal:** La gestión de datos personales a menudo es externalizada, lo que plantea riesgos de privacidad. Blockchain permite una gestión personalizada y segura de datos personales, reduciendo la dependencia de terceros.
7. **Innovaciones en Autenticación y Verificación:** La transición hacia la blockchain abre nuevas posibilidades en la autenticación y verificación de identidades, utilizando tecnologías avanzadas como la biometría, contratos inteligentes y tokens de identidad, que ofrecen un nivel superior de seguridad y eficiencia.

2.4 Resolviendo la problemática de identidad digital con Blockchain

La tecnología blockchain, con su enfoque en la descentralización y distribución de datos, se está estableciendo como una solución pionera para superar los desafíos de seguridad y privacidad inherentes a los sistemas de identidad digital actuales. Su aplicación en este campo promete no solo revolucionar la manera en que creamos, gestionamos y verificamos elementos identificativos en un entorno digital, sino también fortalecer la protección contra ataques y filtraciones de datos al distribuir la información a través de una red de nodos descentralizados. A continuación, exploraremos los aspectos clave de cómo blockchain está facilitando esta transformación, abarcando desde la creación de identificadores únicos hasta la automatización de procesos de gestión de identidades a través de smart contracts [12][15][16]:

- **Creación y registro de DiDs (Identificadores Descentralizados):** La creación y registro de DiDs mediante blockchain representa un avance significativo sobre los sistemas centralizados tradicionales. Estos DiDs son direcciones únicas y verificables en una red distribuida, asegurando que la identidad de un individuo pueda ser verificada de manera confiable, sin depender de intermediarios.
- **Almacenamiento de hash para notarización de credenciales:** La capacidad de blockchain para almacenar hash de credenciales brinda una notarización digital segura y distribuida. Esto garantiza que la información vital sea inmutable y resistente a modificaciones no autorizadas, potenciando la integridad de los datos
- **Consentimiento y derechos de acceso:** Gestionar el acceso a la identidad digital como una transacción en la blockchain permite a los individuos brindar consentimiento y derechos de acceso de manera controlada. Por ejemplo, se podría permitir el acceso a cierta información por un tiempo limitado, revocando el acceso una vez transcurrido el tiempo acordado.
- **Amplias aplicaciones con smart contracts:** Los smart contracts en la blockchain, operando en un entorno descentralizado, habilitan un amplio abanico de posibilidades para la gestión de identidades digitales. Estos contratos automatizan y descentralizan la gestión de consentimientos y verificación, ofreciendo una mayor transparencia y control para el usuario

Blockchain presenta una solución robusta y prometedora para los desafíos persistentes en la gestión de identidades digitales. Su naturaleza descentralizada, junto con la capacidad de proporcionar verificación inmutable y gestión de consentimientos, pone las bases para una nueva era en la gestión de identidades digitales. La implementación de blockchain en la gestión de identidades no solo mejora la seguridad y la privacidad, sino que también permite una mayor autonomía y control sobre la propia identidad en el mundo digital.

2.5 Comprendiendo la identidad descentralizada

La Identidad Descentralizada (DID) se erige como una respuesta a los desafíos asociados con las identidades centralizadas, proporcionando una ruta hacia una gestión de identidad más autónoma y segura. A continuación, se nombran los

elementos centrales que componen la Identidad Descentralizada y cómo estos elementos colaboran para revolucionar la gestión de identidades [12][19].

- **Identificadores Descentralizados según W3C:** El corazón de la identidad descentralizada reside en los Identificadores Descentralizados (DIDs) definidos por el Consorcio World Wide Web (W3C). Los DIDs permiten a cualquier individuo o entidad crear y gestionar su propia identidad sin depender de autoridades centralizadas. Esta autonomía fomenta una mayor privacidad y control sobre la información personal [17].
- **Portabilidad entre Plataformas:** Una de las ventajas clave de los DIDs es su capacidad para soportar múltiples plataformas. Esto significa que los usuarios pueden trasladar sus datos y credenciales de identidad entre diferentes sistemas y aplicaciones, lo cual es un avance significativo hacia la portabilidad y el control de datos.
- **Agentes de Usuarios Diversificados:** El ecosistema de identidad descentralizada alberga diferentes tipos de agentes de usuarios, que van desde aplicaciones convencionales (apps), aplicaciones descentralizadas (Dapps), plataformas WEB3 hasta carteras como Metamask. Estos agentes facilitan la interacción con las infraestructuras de identidad descentralizada, permitiendo a los usuarios gestionar y utilizar sus DIDs de manera efectiva.
- **Solucionador Universal:** En un mundo donde diferentes blockchains podrían alojar DIDs, surge la necesidad de solucionadores universales. Estos son controladores o plugins que actúan como intermediarios, ayudando a determinar en qué blockchain se encuentra almacenado un DID específico. De esta manera, simplifican la tarea de localizar y verificar identidades en un entorno descentralizado.

El concepto de Identidad Descentralizada apunta a restaurar el control y la propiedad de la identidad a manos de los individuos. La incorporación de DIDs, la portabilidad entre plataformas y la interoperabilidad facilitada por los agentes de usuarios y solucionadores universales, constituyen pilares fundamentales en la evolución hacia sistemas de identidad más seguros, privados y controlados por el usuario.

2.6 Navegando hacia la identidad autosoberana con Blockchain

La identidad autosoberana (SSI, por sus siglas en inglés Self-Sovereign Identity) es un enfoque moderno para la gestión de identidades digitales que devuelve el control a los individuos sobre su propia información. A diferencia de las identidades gestionadas centralizadamente, la SSI permite a las personas poseer y controlar su información personal sin la intervención de intermediarios. A continuacion, exploraremos la naturaleza de la SSI y cómo la tecnología blockchain facilita su implementación [20].

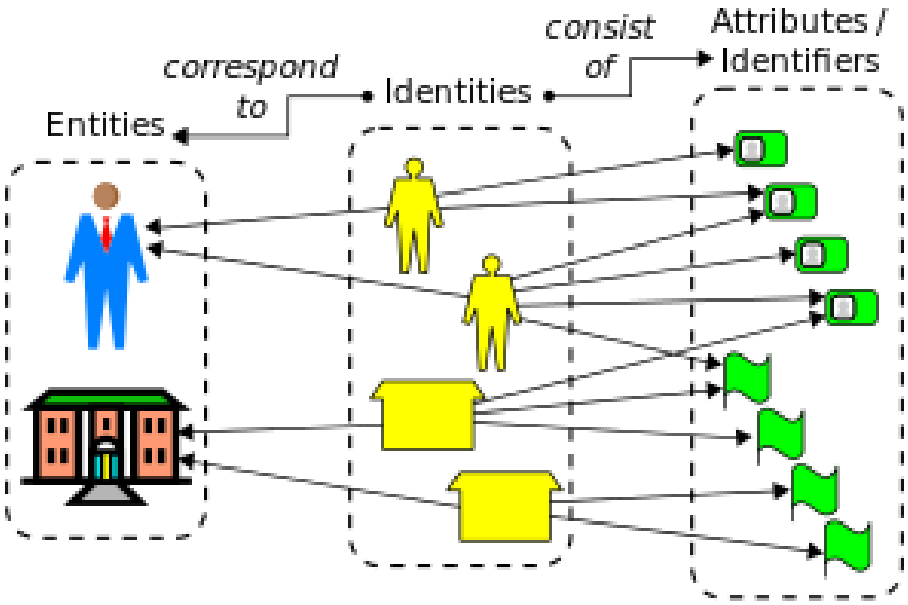


Image from: Auto-identidad soberana - Wikipedia, la enciclopedia libre

Esencia de la identidad autosoberana
La identidad autosoberana resalta la propiedad y el control personal sobre los datos identificativos. En un sistema SSI, los individuos tienen la autoridad para compartir, revocar o verificar su información, reduciendo la dependencia de terceros para la gestión de identidades.
Blockchain como facilitador
La tecnología blockchain se presenta como un facilitador crucial para la implementación de sistemas SSI. Con su capacidad para proporcionar registros inmutables y transparencia, blockchain ofrece una plataforma donde los datos de identidad pueden ser almacenados y verificados de manera segura y eficiente.
Empoderamiento individual
La SSI empodera a los individuos al proporcionar un control total sobre su información. Esto es especialmente relevante en un mundo donde la privacidad y la seguridad de los datos son preocupaciones primordiales. La tecnología blockchain, al ser descentralizada, contribuye a este empoderamiento proporcionando un medio transparente y seguro para gestionar la identidad [21].
Interoperabilidad y portabilidad
La Identidad Autosoberana, apoyada en blockchain, fomenta la interoperabilidad y la portabilidad de datos. Los individuos pueden utilizar su identidad en diferentes plataformas y servicios sin tener que crear nuevas credenciales, lo que simplifica la experiencia del usuario y promueve una gestión de identidad más eficiente.

La Identidad Autosoberana con blockchain propone un futuro donde la confidencialidad, la seguridad y la libertad en la gestión de la identidad digital son alcanzables. Los sistemas SSI, impulsados por blockchain, no solo representan un paso hacia la recuperación de la propiedad de la identidad personal, sino que también establecen un estándar para una gestión de identidad más ética y centrada en el usuario.

2.7. Explorando casos de uso de DIDs

Los Identificadores Descentralizados (DIDs) pueden tener un gran impacto en comunidades y relaciones entre iguales, sin la necesidad de intervención de organismos o entidades centralizadas. En este contexto, los DIDs pueden ser utilizados para fortalecer la autonomía, la privacidad y la seguridad en las interacciones digitales dentro de estas comunidades. Aquí algunos ejemplos de cómo los DIDs podrían aplicarse en este escenario [12]:

1. **Redes Sociales Descentralizadas**: En plataformas de redes sociales gestionadas por la comunidad, los DIDs permitirían a los usuarios controlar su propia identidad digital, mejorando la privacidad y reduciendo la dependencia de plataformas centralizadas que recopilan y monetizan datos de usuario.
2. **Mercados de Trueque y Economía Compartida**: Los DIDs podrían ser utilizados en mercados de trueque o en plataformas de economía compartida para verificar de manera segura y descentralizada la identidad de los participantes, fomentando la confianza y la seguridad en estas transacciones.
3. **Gestión Comunitaria de Recursos**: En comunidades que gestionan recursos compartidos, como cooperativas o asociaciones de vecinos, los DIDs facilitarían la gestión de identidades y accesos, asegurando que solo los miembros autorizados puedan acceder o modificar recursos comunitarios.
4. **Proyectos Colaborativos y Crowdsourcing**: Los DIDs permitirían la verificación y autenticación de contribuyentes en proyectos colaborativos, asegurando la transparencia y la confianza en la contribución y distribución de recursos o créditos dentro de estos proyectos.
5. **Educación y Aprendizaje Colaborativo**: En plataformas de educación descentralizadas, los DIDs podrían utilizarse para verificar la identidad de estudiantes y educadores, facilitando la creación de entornos de aprendizaje seguros y personalizados basados en la confianza mutua.

Estos usos de los DIDs en comunidades y entre iguales reflejan cómo la tecnología puede ser utilizada para potenciar la autonomía, la colaboración y la confianza en entornos descentralizados, complementando y enriqueciendo el panorama de aplicaciones que se menciona en el escenario inicial.

3. Reconocimiento Facial

El reconocimiento facial, tecnología que cumple más de medio siglo, comenzó a gestarse en los años 60 cuando un equipo liderado por Woodrow W. Bledsoe intentó sin éxito que las computadoras reconocieran rostros humanos, topándose con la variabilidad de aspectos como la rotación de la cabeza y la iluminación. Esta área, tradicionalmente desafiante para las computadoras, ha experimentado avances significativos gracias a la mejora en cámaras, procesamiento y aprendizaje automático [22].
Inicialmente, los sistemas de reconocimiento facial se basaban en la tecnología de cámara 2D para mapear puntos nodales del rostro y convertirlos en un código numérico. Sin embargo, esta técnica presentaba limitaciones, como una menor efectividad bajo condiciones de iluminación inadecuadas o movimiento, y era susceptible a ser engañada con fotografías.
Para superar estas debilidades, se han desarrollado sistemas de detección de prueba de vida y redes neuronales convolucionales profundas, que imitan el funcionamiento cerebral en la identificación de patrones en datos de imagen. Ejemplos contemporáneos de esta tecnología se encuentran en dispositivos de consumo masivo como el iPhone XV de Apple, que utiliza una cámara 3D con tecnología infrarroja para mapear patrones faciales.
Actualmente, el reconocimiento facial desempeña un papel crucial en nuestras vidas diarias, revolucionando las economías y sociedades. Se ha convertido en la tecnología predominante para verificar la identidad, aplicada en múltiples escenarios, como la verificación de identidad para registros de usuarios, el acceso a internet, la seguridad de bases de datos y en el sector turístico, entre otros [23].
Debido a estos factores y considerando que la tecnología de reconocimiento facial está al alcance de todos a través de diferentes dispositivos, y que nuestras datos biometricos son únicas e irremplazables, se hace evidente la relevancia de aplicar esta tecnología para resolver problemas complejos. En este capítulo, exploraremos en detalle los diversos modelos de reconocimiento facial pre-entrenados disponibles, seleccionando el más adecuado para nuestras necesidades, discutiremos aspectos técnicos clave y proporcionaremos una visión general de cómo esta tecnología se integrará y funcionará dentro de nuestro sistema. Este análisis nos permitirá comprender mejor no solo la funcionalidad de estos modelos sino también como implementarlo.

3.1 Modelos pre-entrenados para el reconocimiento facial

Ahora es momento de hablar sobre el ámbito del reconocimiento facial y los diferentes modelos pre-entrenados de inteligencia artificial que facilitan la implementación de esta tecnología. A continuación, se describen algunos de estos modelos junto con enlaces a recursos adicionales para obtener más información:

1. **Inception ResNet (V1):**
    - El modelo Inception ResNet (V1), desarrollado por investigadores de Google, ha mostrado un rendimiento sobresaliente en tareas de reconocimiento facial. Este modelo ha sido pre-entrenado en datasets extensos, lo que permite identificar características faciales importantes [24].
2. **VGGModels (VGGFace1 y VGGFace2):**

- Los modelos VGGFace1 y VGGFace2, desarrollados por el Visual Geometry Group de Oxford, proporcionan arquitecturas pre-entrenadas que han demostrado ser efectivas para el reconocimiento facial. Al estar entrenados en grandes datasets, proporcionan un punto de partida robusto para aplicaciones que buscan comparar datos biométricos [25].

3. **DeepFace (Facebook):**
    - DeepFace, desarrollado por Facebook, es un modelo altamente avanzado con una estructura de red profunda que permite un alto grado de precisión en la identificación facial [26].
4. **Modelos del Visual Geometry Group (VGG) de Oxford (VGG-16, ResNet-50, y SeNet-50):**
    - Los modelos del Visual Geometry Group de Oxford, incluyendo VGG-16, ResNet-50, y SeNet-50, están diseñados específicamente para tareas de reconocimiento y clasificación facial. En particular, el modelo VGG-16 se caracteriza por su estructura simple y clara, lo que facilita su implementación y adaptación [27].
5. **FaceNet:**
    - FaceNet, desarrollado por Google, es un modelo pre-entrenado que utiliza una métrica de distancia para comparar las imágenes faciales [28].

Tras revisar los diferentes modelos pre-entrenados para el reconocimiento facial, el modelo FaceNet de Google parece ser el mas adecuado. FaceNet destaca por su capacidad de generar embeddings (representaciones numéricas) de imágenes faciales que luego pueden ser comparadas mediante una métrica de distancia, facilitando así la verificación de la identidad basada en la similitud facial.

En nuestro caso se busca una autenticación fluida y precisa mediante el reconocimiento facial. Al registrar un nuevo usuario, se capturarán imágenes desde diferentes ángulos utilizando la webcam, y FaceNet generará embeddings correspondientes que se almacenarán en la base de datos. Posteriormente, en el momento del inicio de sesión, se capturará una nueva imagen, se generará el embedding correspondiente y se comparará con los embeddings almacenados para verificar la identidad del usuario [29].

3.2 FaceNet: Un modelo pre-entrenado para reconocimiento facial

FaceNet es un sistema de reconocimiento facial desarrollado por investigadores de Google en 2015, que en su momento logró resultados líderes en el sector en una variedad de conjuntos de datos benchmark de reconocimiento facial [29]. La propuesta original de FaceNet fue publicada en un documento titulado "FaceNet: A Unified Embedding for Face Recognition and Clustering" donde se lograron resultados de vanguardia en muchos conjuntos de datos de reconocimiento facial de referencia. A continuación, se describen los aspectos más relevantes de FaceNet

3.2.1 Introducción a FaceNet

FaceNet es una arquitectura innovadora desarrollada por investigadores de Google en 2015, que estableció un nuevo estándar en el campo del reconocimiento facial, logrando resultados notables en varios benchmarks reconocidos en la comunidad científica. Utilizando técnicas de aprendizaje profundo, FaceNet proporciona un enfoque robusto y efectivo para la identificación y verificación facial. A continuación, se presentan los aspectos clave de FaceNet que lo distinguen en el ámbito del reconocimiento facial [30].

- **Arquitectura de FaceNet**

  La arquitectura de FaceNet es una red neuronal que procesa las imágenes faciales y las convierte en vectores característicos en un espacio multidimensional. Por lo tanto, las imágenes de la misma persona tendrán vectores cercanos entre sí, mientras que las de diferentes personas estarán más separadas en este espacio multidimensional [31].

- **Implementaciones**

  Dada la popularidad y la eficacia demostrada de FaceNet, existen varias implementaciones abiertas al público.

- **Aplicaciones**

  FaceNet tiene un amplio rango de aplicaciones que incluyen sistemas de seguridad y vigilancia, aplicaciones en redes sociales, y plataformas de comercio electrónico donde la identificación y verificación facial es crucial.

En resumen, FaceNet ofrece una solución robusta y eficiente para el reconocimiento facial. De hecho se realizo un estudio donde se probo la velocidad para detectar rostros en un conjunto de 300 imágenes en un mismo dispositivo y se obtuve el siguiente resultado.

Package	FPS (1080x1920)	FPS (720x1280)	FPS (540x960)
facenet-pytorch	12.97	20.32	25.50
facenet-pytorch (non-batched)	9.75	14.81	19.68
dlib	3.80	8.39	14.53
mtcnn	3.04	5.70	8.23

Es notable cómo la eficacia de FaceNet en la detección de rostros se incrementa significativamente con la mejora en la calidad de los dispositivos de reconocimiento facial. Esta correlación resalta la importancia de utilizar hardware de alta calidad para optimizar la precisión y el rendimiento de sistemas avanzados de reconocimiento facial como FaceNet

3.2.2 Arquitectura de FaceNet

FaceNet es una arquitectura revolucionaria que se ha desarrollado para abordar desafíos en el reconocimiento facial utilizando aprendizaje profundo. Su arquitectura única permite la transformación de imágenes faciales en un espacio vectorial, facilitando la comparación y reconocimiento de rostros. A continuación, se describen los componentes clave y características de esta arquitectura [32][33]:

- **Arquitectura con red neuronal convolucional (CNN)**
  FaceNet emplea una arquitectura de red neuronal convolucional (CNN) que permite la extracción eficaz de características faciales. Las CNN son especialmente potentes en la identificación de patrones jerárquicos en imágenes.
- **Normalización L2**
  Los embeddings generados son normalizados utilizando la normalización L2, lo que asegura que las representaciones vectoriales tengan una longitud unitaria en el espacio métrico. Esto ayuda a mantener las distancias consistentes y comparables, facilitando la tarea de reconocimiento facial.
- **Embedding de imágenes**
  FaceNet está diseñado para transformar las imágenes faciales en un espacio vectorial donde las distancias entre los vectores corresponden a las similitudes entre las imágenes faciales. Esta representación vectorial facilita la comparación y reconocimiento de rostros.
- **Triplet Loss**
  FaceNet introduce un tipo de función de pérdida denominada "Triplet Loss", que es esencial para su desempeño eficaz. Esta función de pérdida busca minimizar la distancia entre las imágenes de la misma persona y maximizar la distancia entre imágenes de personas diferentes.

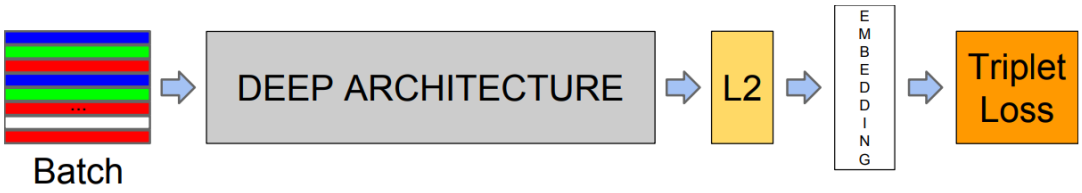


Image from: [Detailed explaination of Facenet Model]

La arquitectura de FaceNet, con su enfoque en la optimización de la función de Triplet Loss y la transformación efectiva de imágenes faciales en un espacio vectorial, ha establecido un nuevo estándar en el campo del reconocimiento facial. Su capacidad para generar representaciones vectoriales precisas y eficaces lo hace una elección robusta para aplicaciones de reconocimiento facial y verificación de identidad.

3.2.3 Ventajas de FaceNet para la Autenticación Facial

La arquitectura de Facenet lo hace apto para aplicaciones que requieren una autenticación facial precisa y robusta. A continuación, se detallan las ventajas de utilizar FaceNet para la autenticación facial en la plataforma propuesta [34][35]:

1. **Capacidad de Identificación**: FaceNet demuestra una notable competencia en identificar caras similares a través de diversas

expresiones faciales y ángulos, lo que es crucial para una plataforma que se apoya en la autenticación facial para el registro y el inicio de sesión.
2. **Flexibilidad**: FaceNet puede ser implementado de manera que las imágenes capturadas en tiempo real a través de una webcam puedan ser procesadas y comparadas con las imágenes almacenadas en una base de datos. Esta flexibilidad es esencial para una funcionalidad de inicio de sesión eficaz en la plataforma propuesta.
3. **Desempeño en Varias Condiciones**: La habilidad de FaceNet para operar eficazmente bajo diversas condiciones, como cambios en la iluminación y obstrucciones, lo hacen adecuado para un entorno donde los usuarios podrían estar iniciando sesión bajo una variedad de condiciones.
4. **Implementación Pre-entrenada**: La disponibilidad de implementaciones pre-entrenadas de FaceNet reduce la barrera de entrada para integrar esta tecnología en la plataforma. Por ejemplo, es posible probar el modelo en VectorHub con solo 3 líneas de código Python, permitiendo una rápida integración y prueba del modelo en la plataforma.
5. **Mejora Continua**: Aunque FaceNet tiene algunas debilidades, como la dificultad para encontrar buenas coincidencias si la imagen está editada con palabras en frente o si los individuos llevan gafas, existe la posibilidad de mejorar el modelo re-entrenándolo con un dataset que tenga más imágenes con una mayor variedad de etnias, gafas y distorsiones. Esta característica de mejora continua sugiere que FaceNet puede evolucionar y adaptarse a las necesidades cambiantes de la plataforma propuesta.

Las ventajas mencionadas resaltan la aptitud de FaceNet como un modelo pre-entrenado viable para la autenticación facial en la plataforma propuesta. Sin embargo, es imperativo considerar que la efectividad del modelo puede variar según la implementación específica y el dataset utilizado para el entrenamiento o re-entrenamiento del modelo.

3.3 Implementación

Etapa inicial

Iniciaremos la implementación de FaceNet con pruebas en un entorno local, enfocándonos en comprender el funcionamiento del modelo y ajustar parámetros. Utilizaremos un conjunto limitado de datos para evaluar la capacidad del modelo en la identificación y verificación de rostros y para solucionar problemas relacionados con la detección y procesamiento de imágenes faciales. El objetivo es garantizar la robustez y fiabilidad del modelo antes de integrarlo en entornos más complejos.

Integración con el front-end

La integración de FaceNet en el front-end de nuestra aplicación se centrará en desarrollar una interfaz de usuario intuitiva y funcional. Esta interfaz facilitará el proceso de registro facial, proporcionando indicaciones claras y

retroalimentación en tiempo real para una experiencia de usuario fluida y eficaz, manteniendo la precisión del modelo.

Desarrollo del back-end

Simultáneamente, desarrollaremos la lógica del back-end para procesar y manejar los datos capturados por el front-end. Estableceremos protocolos para la captura y almacenamiento de imágenes faciales y embeddings, y reforzaremos la seguridad para proteger los datos biométricos de los usuarios.

Objetivo final

La integración de FaceNet en nuestro proyecto tiene como objetivo final establecer un sistema de registro y autenticación basado en reconocimiento facial, con los siguientes apartados concretos:

1. **Registro Facial**: Los usuarios registrarán sus rostros capturando imágenes desde varios ángulos. FaceNet procesará estas imágenes para generar embeddings faciales.
2. **Almacenamiento en la Base de Datos**: Los embeddings generados se almacenarán de forma segura en nuestra base de datos, asociándolos con los perfiles de usuario correspondientes.
3. **Inicio de Sesión**: Durante el inicio de sesión, el sistema capturará una nueva imagen del usuario y la comparará con los embeddings almacenados en la base de datos.
4. **Visualización del Perfil de Usuario**: Si el sistema reconoce al usuario a través de la coincidencia de embeddings, se otorgará acceso y se mostrará el perfil de usuario correspondiente.

De esta forma, conseguiremos montar la estructura y la implementación del reconocimiento facial adecuadamente, estableciendo un sistema de autenticación seguro y preciso.

4. Substrate

4.1 Introducción a Substrate

Substrate es un marco de desarrollo (framework) de blockchain creado con el objetivo de proporcionar una plataforma flexible, abierta, interoperable y a prueba de futuro para los desarrolladores. La idea es que los desarrolladores puedan construir sobre una estructura de blockchain específicamente optimizada para sus requerimientos, que evoluciona de manera fluida con sus necesidades sin necesidad de realizar bifurcaciones (forks) en el código. Este framework fue desarrollado por el equipo de Parity, que también ha trabajado en software blockchain para Ethereum y la red Polkadot. Substrate fue usado por Parity para construir la red Polkadot, lo que refleja su alta flexibilidad y robustez [36][37].
El origen de Substrate proviene de la visión de superar las limitaciones encontradas en las redes de blockchain de generaciones anteriores. Los pioneros y veteranos de la industria blockchain que desarrollaron Substrate, encontraron que, al construir clientes en los primeros días de Bitcoin y Ethereum, estaban recreando mucha de la misma funcionalidad, pero con diferentes limitaciones en torno a la escala, gobernanza, bifurcaciones, interoperabilidad y actualizaciones. Substrate nació de la visión de que los desarrolladores no deberían tener que recrear los fundamentos al construir y optimizar una blockchain.
En el contexto de la blockchain, Substrate surge como una solución para hacer la construcción de blockchains más segura, económica, fácil y rápida. Permite a los usuarios iniciar el desarrollo sin invertir mucho tiempo en la configuración de la cadena, génesis y consenso, todo lo cual es posible mediante la configuración en un archivo JSON. Además, Substrate se describe como un framework para construir blockchains, encargándose de la mayoría de las tareas pesadas relacionadas con el consenso, la red peer-to-peer (P2P), la gestión de cuentas, la lógica básica de blockchain, y proporcionando un cliente para interactuar con la blockchain [38][39].
Por este motivo, blockchain nos permitirá almacenar las identidades de forma anónima, transparentes, … A continuación, hablaremos sobre las características que componen substrate, su arquitectura, los beneficios de blockchain en profundidad y después hablaremos sobre como funcionan los pallets que es como y como funciona y por ultimo cual será nuestra implementacion

4.2 Características Clave de Substrate

Modularidad y extensibilidad:
Substrate es un framework modular que permite a los desarrolladores seleccionar y cambiar componentes según sea necesario, como la pila de red o el motor de consenso. Esta flexibilidad facilita la adaptación del framework a las necesidades específicas de cada proyecto, permitiendo un desarrollo de blockchain altamente personalizable. [40][41]
Framework para contratos inteligentes:
Substrate ofrece un entorno robusto para el desarrollo y despliegue de contratos inteligentes. Soporta tanto WebAssembly como contratos compatibles con EVM, proporcionando herramientas y lenguajes diversos para la creación de contratos.

Incluye módulos específicos, como el Pallet de Contratos y el Pallet EVM, para facilitar la implementación de lógicas de contratos inteligentes. [42][43]

Capacidad de personalización:

Substrate permite la personalización profunda de redes blockchain para satisfacer necesidades empresariales específicas. Esto incluye la implementación de mecanismos de consenso personalizados y modelos de gobernanza. Utilizando el FRAME de Substrate, los desarrolladores pueden seleccionar o construir pallets personalizados, ofreciendo una gran libertad de configuración. [44][45]

Interoperabilidad con otras blockchains:

Substrate asegura una interoperabilidad eficiente con otras blockchains. Mediante el uso de Mensajería Cross-Consensus (XCM), facilita la comunicación entre blockchains basadas en Substrate. Además, las blockchains construidas con Substrate pueden funcionar como cadenas independientes o integrarse en redes más grandes como Polkadot para una mayor interoperabilidad con otras plataformas blockchain. [46][47]

4.3 Arquitectura de Substrate

La arquitectura de Substrate se compone de varios componentes que facilitan la construcción de blockchains personalizadas. Los componentes principales incluyen el Núcleo de Substrate, el FRAME (Framework for Runtime Aggregation of Modularized Entities) y los pallets que son módulos que se pueden utilizar para agregar funcionalidades específicas a la blockchain [48][49].

1. **Núcleo de Substrate:**
    - **Cliente de Substrate:** Es la implementación en Rust de la lógica de blockchain que se ejecuta en cada nodo de la red.
    - **Runtime de Substrate:** Es el código que se ejecuta en la cadena de bloques y se compila a WebAssembly (Wasm) para garantizar la portabilidad entre diferentes sistemas.
2. **FRAME:**
    - FRAME es un framework que facilita la creación de runtimes personalizados utilizando una amplia variedad de pallets predefinidos o personalizados.
3. **Pallets:**
    - Los pallets son módulos reutilizables que encapsulan una funcionalidad específica y se pueden combinar para formar un runtime de blockchain completo.

El runtime es el corazón de la blockchain en Substrate, y define la lógica que se ejecuta en la cadena. Se compila en WebAssembly, lo que permite una ejecución consistente en diferentes sistemas y garantiza que todos los nodos ejecuten el mismo código validado.

1. **Módulos de runtime (Pallets):**
    - Los pallets son los módulos que componen el runtime, y cada uno encapsula una funcionalidad específica como gestión de balances, contratos inteligentes, o mecanismos de consenso.
    - Los pallets pueden ser desarrollados por la comunidad, lo que permite una extensibilidad y personalización enormes.
2. **Configuración del Runtime:**

- Los desarrolladores pueden configurar su runtime seleccionando pallets existentes o creando nuevos pallets para satisfacer sus necesidades específicas.

El sistema de consenso es crucial para la operación segura y eficiente de la blockchain, y Substrate proporciona una variedad de mecanismos de consenso que los desarrolladores pueden elegir o personalizar según sus necesidades.

1. **Mecanismos de Consenso:**
    - Substrate soporta varios mecanismos de consenso incluyendo Proof of Work (PoW), Proof of Stake (PoS), y otros mecanismos híbridos.
    - Los mecanismos de consenso pueden ser seleccionados y configurados en función de las necesidades del proyecto.
2. **Finalización:**
    - La finalización es un proceso que garantiza la irreversibilidad de los bloques una vez alcanzado un consenso, lo que proporciona seguridad contra ataques y forks malintencionados.
    - Substrate ofrece finalizadores como GRANDPA que proporcionan finalización eficiente y segura para las blockchains.

Esta arquitectura modular y extensible, junto con el soporte para una amplia variedad de mecanismos de consenso y finalización, hacen de Substrate una plataforma poderosa y flexible para el desarrollo de blockchains personalizadas.

4.4 Implementación con Pallets

Los pallets en Substrate son componentes esenciales que proporcionan funcionalidades específicas para la construcción de blockchains. Cada pallet es un módulo basado en Rust que se integra en el runtime de una blockchain, permitiendo a los desarrolladores agregar o modificar características sin necesidad de reescribir el código desde cero. Estos pallets son fundamentales para la flexibilidad y eficiencia de Substrate, ya que permiten una personalización detallada y un desarrollo más ágil.

En nuestro proyecto, emplearemos los pallets para crear una funcionalidad de prueba de existencia (proof of existence). Esta característica es crucial para nuestro sistema de almacenamiento de identidades, ya que nos permitirá registrar y verificar la existencia de un hash de usuario en la blockchain. La implementación de un pallet de prueba de existencia nos facilitará crear y eliminar claims (reclamaciones), asegurándonos de que el hash de cada usuario exista y sea verificable en la blockchain.

El proceso comienza con la creación de un pallet personalizado para gestionar los claims. Este pallet permitirá a los usuarios registrar un hash, que representa su identidad o información relevante, en la blockchain. Cuando un usuario crea un claim, el hash se registra y se almacena en la blockchain, proporcionando una evidencia inmutable y transparente de su existencia.

Además de crear claims, el pallet también proporcionará la funcionalidad para eliminarlos. Esto es importante para mantener la relevancia y exactitud de la información en la blockchain. Los usuarios podrán eliminar sus claims cuando ya no sean necesarios o cuando deseen actualizar su información. Esta capacidad asegura que la blockchain refleje solo la información actual y relevante.

La implementación de este pallet de prueba de existencia no solo garantiza la seguridad y la transparencia en el manejo de la información de identidad, sino

que también brinda a los usuarios el control sobre sus datos. Al almacenar los hashes en la blockchain, se proporciona una capa adicional de seguridad y se evita la manipulación o el acceso no autorizado a la información.
En resumen, el uso de pallets en Substrate para implementar una funcionalidad de prueba de existencia nos permitirá manejar de forma eficiente y segura las identidades de los usuarios en nuestra blockchain. Esta implementación será un componente clave en nuestro proyecto, asegurando la transparencia, la seguridad y el control por parte de los usuarios sobre sus propios datos.

5. Descripción, documentación y Ejecución del proyecto

Ahora nos centramos en desarrollar un sistema de identidad digital integrando blockchain con Substrate y reconocimiento facial en Django y Python.

Para empezar este es el enlace al repositorio de git:

https://github.com/FrankC013/TerritoryId.git

5.1 Estructura del proyecto

El proyecto se centra en la implementación de un sistema de identidad digital utilizando blockchain y reconocimiento facial, aprovechando las capacidades de la tecnología Substrate. La estructura del proyecto ha sido diseñada para facilitar la comprensión, el desarrollo y la escalabilidad. La estructura principal del repositorio se organiza de la siguiente manera:

territoryId: Este es el directorio principal y se centra en la gestión de identidades y el procesamiento de reconocimiento facial. Incluye subdirectorios tanto para almacenar datos de reconocimiento facial hasta manejar la migración de la base de datos y la presentación de interfaces de usuario. Ha sido desarrollado con Django, Python, Javascript y CSS. Es el corazón del proyecto

substrate-front-end-template: Esta plantilla permite crear una aplicación front-end que se conecta al back-end de un nodo Substrate con una configuración mínima. Esta plantilla esta creado con la aplicación Create React y la API Polkadot JS.

substrate-node-template: Esta modulo aloja la lógica de la blockchain y los módulos necesarios para la gestión de los nodos. Ha sido desarrollado principalmente con Rust.

Archivos de Configuración, Entorno y Documentación: Encontraremos archivos como Cargo.toml y manage.py que facilitan la gestión de dependencias, variables de entorno y tareas administrativas, asegurando que el sistema sea fácil de configurar y ejecutar. Por otro lado, los archivos README.md ofrecerán una guía sobre como instalar, configurar y utilizar el sistema.

Con esta estructura, nos aseguramos de que cada componente del sistema esté organizado lógicamente y sea fácilmente accesible y escalable, lo que facilita el mantenimiento y la colaboración en el proyecto.

5.2 Configuración y preparación del entorno

Para garantizar una correcta ejecución, es fundamental instalar las dependencias y librerías especificadas en el archivo test-requirements.txt. Este archivo contiene una lista de todos los paquetes necesarios para realizar pruebas

de software de manera efectiva. A continuación, se detalla el proceso de instalación:

Preparación del Entorno de Trabajo:
Antes de proceder con la instalación, asegúrate de tener Python instalado en tu sistema. Este proyecto requiere Python 3.9.
Se recomienda utilizar un entorno virtual para la instalación de paquetes, lo que ayuda a mantener las dependencias del proyecto separadas y organizadas. Puedes crear un entorno virtual utilizando herramientas como **venv** o **conda**.

Instalación de Dependencias:
Navega hasta la raíz del repositorio donde se encuentra el archivo test-requirements.txt.
Ejecuta el comando:

```
(venv) PS C:\Users\fcron\Documents\PycharmProjects\TerritoryId> pip install -r test-requirements.txt
Collecting face_recognition
  Downloading face_recognition-1.3.0-py2.py3-none-any.whl (15 kB)
Collecting opencv-python
```

Este comando instalará automáticamente todas las dependencias enumeradas en el archivo.

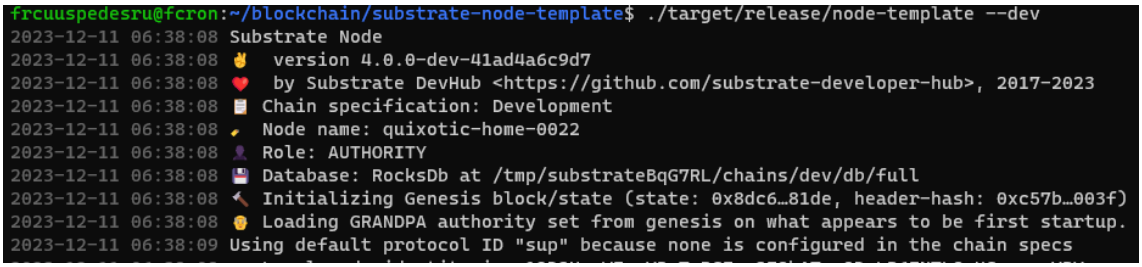
Verificación:
Una vez completada la instalación, puedes verificar que todas las dependencias se hayan instalado correctamente mediante el comando pip freeze. Este comando listará todos los paquetes instalados en el entorno virtual.

```
(venv) PS C:\Users\fcron\Documents\PycharmProjects\TerritoryId> pip freeze
filelock==3.13.1
fsspec==2023.10.0
Jinja2==3.1.2
MarkupSafe==2.1.3
mpmath==1.3.0
networkx==3.2.1
sympy==1.12
torch==2.1.1
typing_extensions==4.8.0
(venv) PS C:\Users\fcron\Documents\PycharmProjects\TerritoryId>
```

5.2.1 Configuración del Substrate Node Template

Es momento de configurar los nodos de Substrate, una parte esencial del proyecto. Este apartado detalla los pasos para configurar y ejecutar un nodo de Substrate.

1. Preparación del Entorno: Primero, verifica que tu sistema cumpla con los requisitos de Rust y otros paquetes necesarios para compilar el template de Substrate.
2. Construcción del Nodo: utiliza cargo build --release para compilar el nodo sin iniciar su ejecución. Este comando prepara el nodo para su uso.
3. Ejecución de la Cadena de Desarrollo en un Solo Nodo: Puedes iniciar una cadena de desarrollo en un solo nodo para pruebas y desarrollo con:



Y limpiar el estado de la cadena de desarrollo con:

Estructura del Substrate Node Template

El proyecto se compone de varios componentes distribuidos en diferentes directorios, esenciales para la configuración y funcionamiento de los nodos de Substrate:

- Node: Contiene la lógica del nodo blockchain, incluyendo la especificación de la cadena (chain_spec.rs) y la definición del servicio del nodo (service.rs).
- Runtime: Usa FRAME para construir la lógica del runtime del blockchain, con módulos llamados "pallets" para definir la lógica del dominio específico.
- Pallets: El runtime se construye con varios pallets de FRAME, proporcionando funciones como el almacenamiento, dispatchables, eventos y manejo de errores.

Se puede encontrar mas documentacion en la pagina oficial de substrate-

5.2.2 Configuración del Substrate Front End Template

Esta plantilla facilita la creación de aplicaciones front-end para interactuar con un back-end de nodo Substrate. Este apartado detalla los pasos para la instalación y configuración del template.

1. Instalación Local: Asegúrate de tener instalado git y yarn globalmente en tu sistema.
2. Uso del Template: Para iniciar el template en modo de desarrollo y conectarlo a un nodo local, usa el comando yarn start.
3. Versión Alojada: Para conectar con tu nodo local Substrate, utiliza el enlace proporcionado.

```
Compiled successfully!

You can now view substrate-front-end-template in the browser.

  Local:            http://localhost:8000/substrate-front-end-template
  On Your Network:  http://192.168.211.180:8000/substrate-front-end-template

Note that the development build is not optimized.
To create a production build, use yarn build.

assets by path static/media/ 1.66 MiB
  assets by path static/media/*.svg 982 KiB 3 assets
  assets by path static/media/*.eot 230 KiB 3 assets
  assets by path static/media/*.ttf 230 KiB 3 assets
  assets by path static/media/*.woff 126 KiB 3 assets
  assets by path static/media/*.woff2 104 KiB
    asset static/media/brand-icons.278156e41e0ad908cf7f.woff2 53.2 KiB [emitted] [immutable] [from: node_modules/semanti
c-ui-css/themes/default/assets/fonts/brand-icons.woff2] (auxiliary name: main)
    + 2 assets
  asset static/media/flags.99f63ae7a743f21ab308.png 27.5 KiB [emitted] [immutable] [from: node_modules/semantic-ui-css/t
hemes/default/assets/images/flags.png] (auxiliary name: main)
asset static/js/bundle.js 8 MiB [emitted] (name: main) 1 related asset
asset index.html 2.27 KiB [emitted]
asset asset-manifest.json 2.1 KiB [emitted]
orphan modules 670 KiB [orphan] 637 modules
runtime modules 28.7 KiB 15 modules
modules by path ./node_modules/ 5.86 MiB (javascript) 1.66 MiB (asset) 1658 modules
modules by path ./src/ 95.5 KiB
  javascript modules 95.4 KiB 19 modules
  json modules 128 bytes 2 modules
modules by mime type application/x-font-ttf 16.3 KiB
  data:application/x-font-ttf;charset=utf-8;base64,AAEAAAAOAIAAAwBg.. 5.71 KiB [built] [code generated]
  + 3 modules
modules by mime type application/font-woff 14.6 KiB
  data:application/font-woff;charset=utf-8;base64,d09GRgABAAAAAAAoU.. 3.41 KiB [built] [code generated]
  data:application/font-woff;charset=utf-8;base64,d09GRk9UVE8AAASw.. 1.61 KiB [built] [code generated]
  + 2 modules
.. 1.29 KiB [built] [code generated]
buffer (ignored) 15 bytes [optional] [built] [code generated]
webpack 5.76.1 compiled successfully in 17454 ms
```

5.3 Despliegue y Ejecución

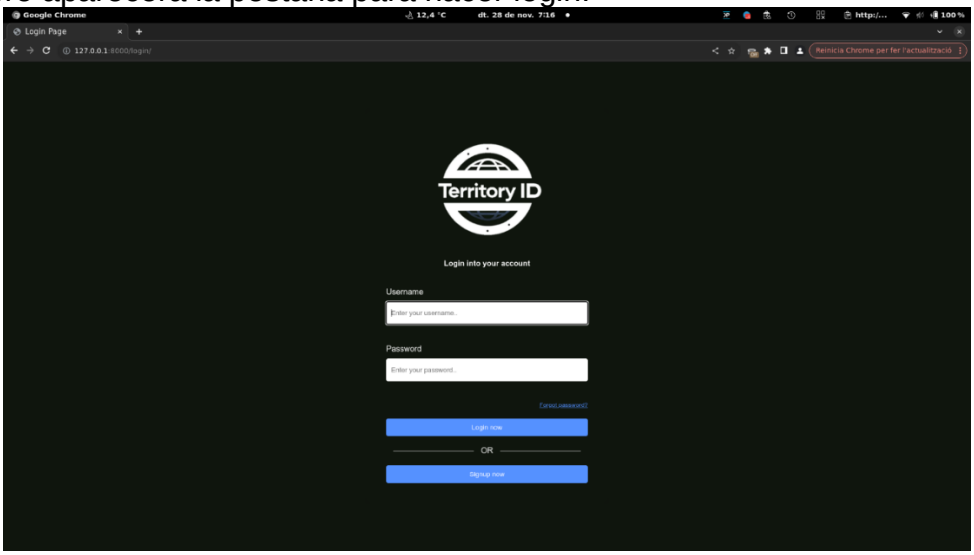
Ahora nos centraremos en el despliegue y ejecución del sistema, explicando los pasos cruciales para poner en marcha el proyecto y utilizar sus funciones de identidad digital y reconocimiento facial. A continuación, se describen los pasos necesarios para el despliegue y la interacción con el sistema.

Primero, necesitas iniciar el servidor web del proyecto. Para esto, ejecuta:

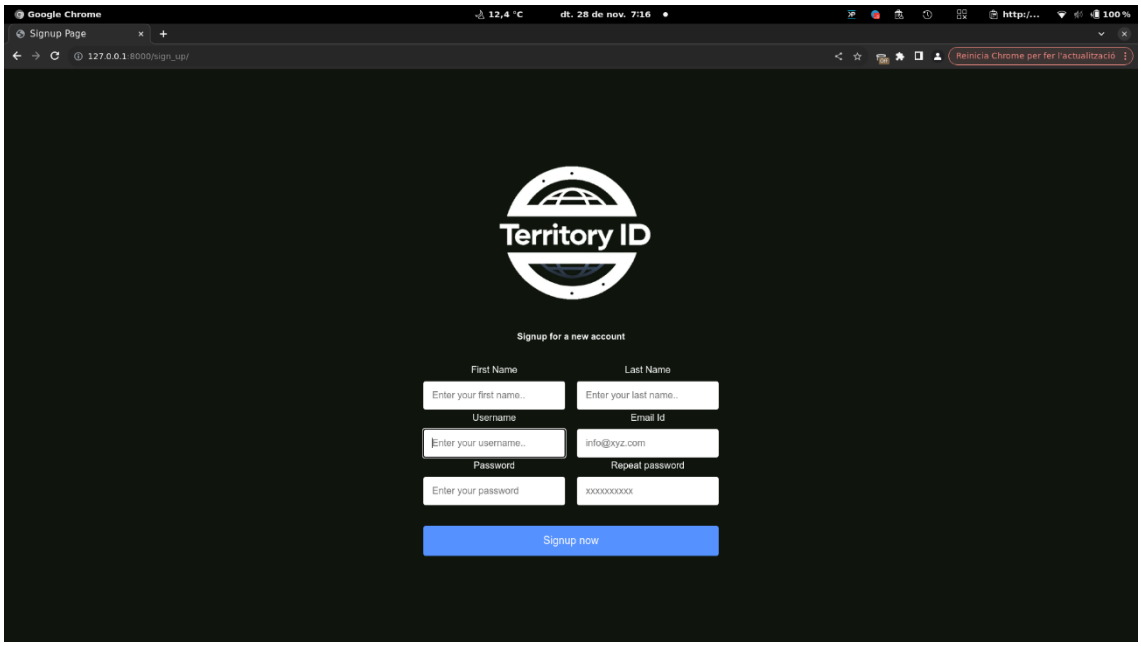
```
(venv) PS C:\Users\fcron\Documents\PycharmProjects\TerritoryId\territoryId> python manage.py runserver
```

Este comando pone en funcionamiento el servidor web y permite acceder a la aplicación a través del navegador.

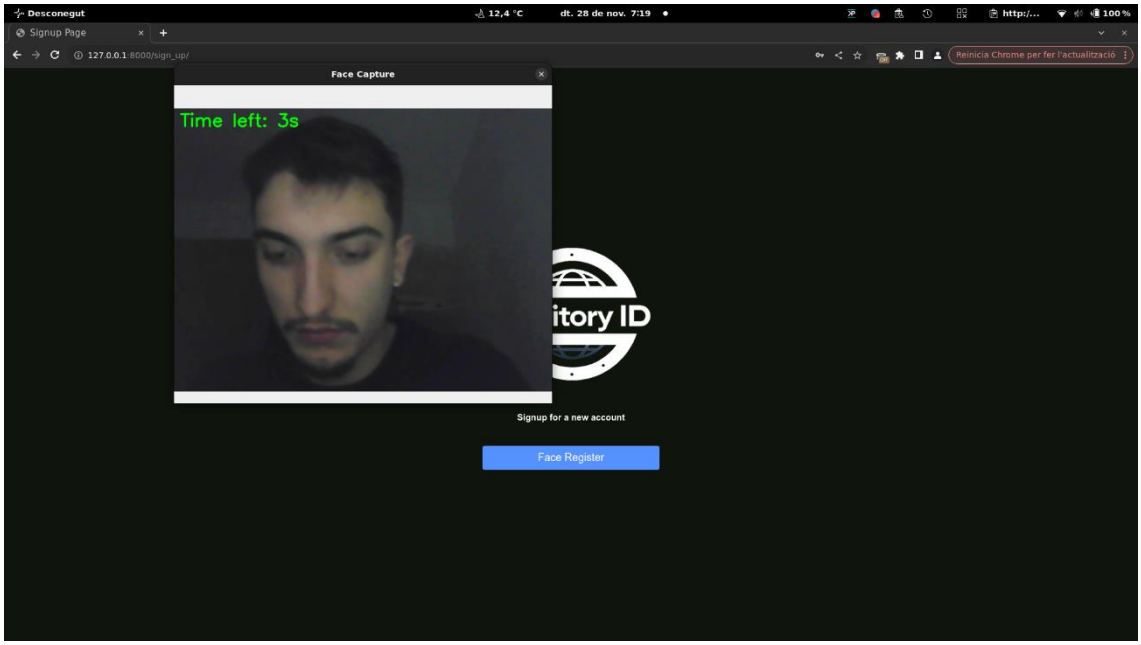
Primero aparecerá la pestaña para hacer login:



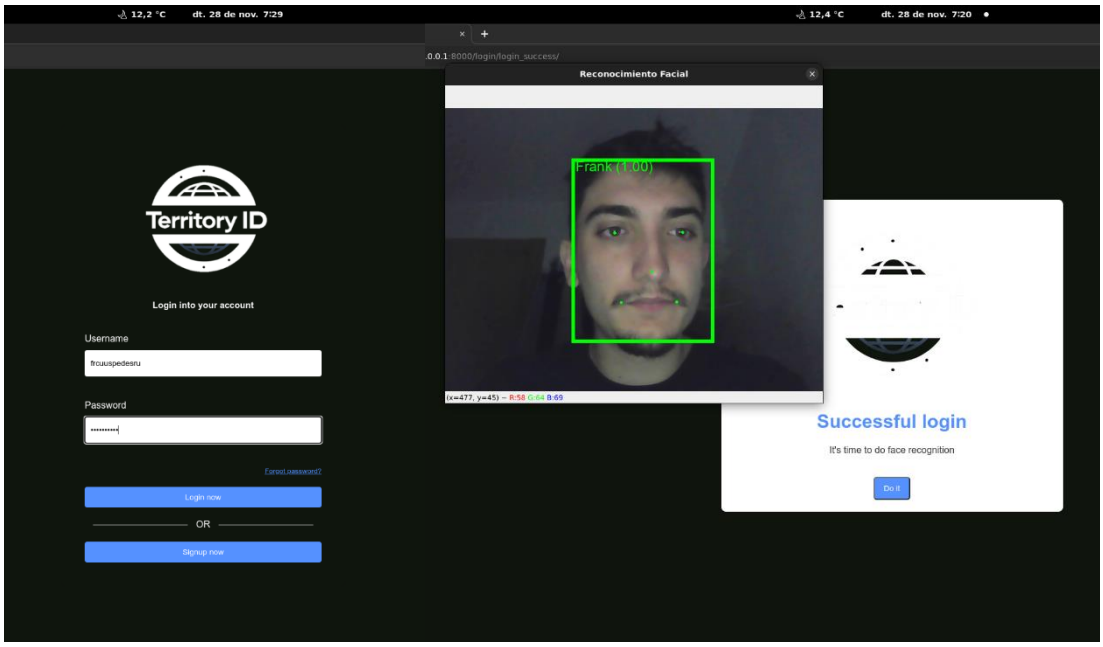
Ahora es momento de realizar el registro. Rellena los campos requeridos en el formulario de registro. Esto incluye información básica como nombre de usuario, correo electrónico y contraseña.



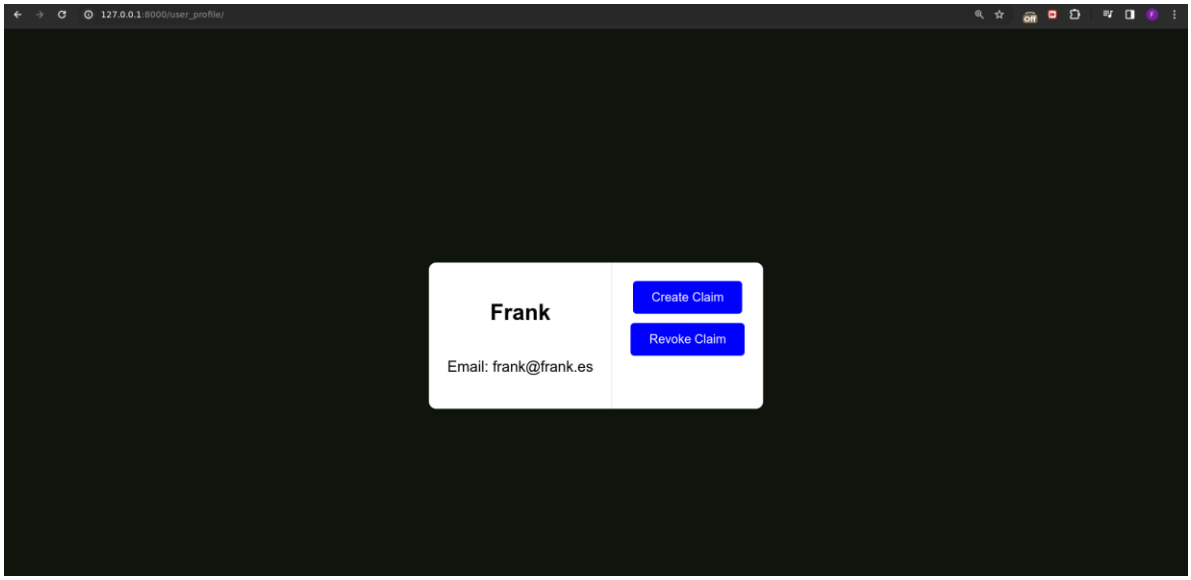
Una vez realizado el registro correctamente es momento de hacer el registro facial:



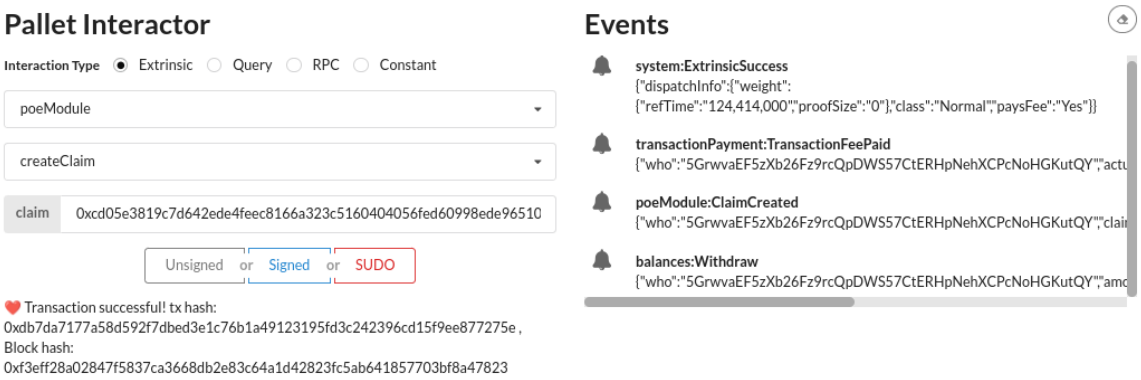
A partir de este punto ya puedes realizar el login con el reconocimiento facial:



Una vez se ha realizado el login se accederá al perfil de usuario donde se podrá crear una transaccion enlazada con tu cuenta en la blockchain de polkadot con tu propio nodo local.



Una vez creado se puede acceder al front-end de substrate para ver la existencia de la transaccion.


Pallet Interactor
Interaction Type
Extrinsic
Query
RPC
Constant
poeModule
createClaim
claim
0xcd05e3819c7d642ede4feec8166a323c5160404056fed60998ede96510
Unsigned
or
Signed
or
SUDO
❤️ Transaction successful! tx hash:
0xdb7da7177a58d592f7dbed3e1c76b1a49123195fd3c242396cd15f9ee877275e ,
Block hash:
0xf3eff28a02847f5837ca3668db2e83c64a1d42823fc5ab641857703bf8a47823
Events
system:ExtrinsicSuccess
{"dispatchInfo":{"weight":
{"refTime":"124,414,000","proofSize":"0"},"class":"Normal","paysFee":"Yes"}}
transactionPayment:TransactionFeePaid
{"who":"5GrwvaEF5zXb26Fz9rcQpDWS57CtERHpNehXCPcNoHGKutQY","actu
poeModule:ClaimCreated
{"who":"5GrwvaEF5zXb26Fz9rcQpDWS57CtERHpNehXCPcNoHGKutQY","clai
balances:Withdraw
{"who":"5GrwvaEF5zXb26Fz9rcQpDWS57CtERHpNehXCPcNoHGKutQY","amo

6. Conclusiones y trabajos futuros

6.1 Resumen de Conclusiones

En el desarrollo de este proyecto, me he enfrentado a varios desafíos significativos, cada uno aportando valiosas lecciones y perspectivas.

- **Desafíos de Implementación en Blockchain**: Uno de los aspectos más desafiantes ha sido la implementación de soluciones en blockchain. La naturaleza compleja y en constante evolución de la tecnología blockchain presenta una curva de aprendizaje exponencial. Navegar por este terreno en constante cambio requiere no solo un conocimiento técnico profundo sino también una capacidad para adaptarse rápidamente a nuevas herramientas y prácticas.
- **Programación en Substrate**: Trabajar con Substrate, un framework relativamente nuevo y en constante actualización, ha sido particularmente desafiante. La falta de una base estable de conocimiento y la rápida obsolescencia de los tutoriales / documentación (lo que era nuevo hace 3 meses a 1 año ya está anticuado) han añadido una capa adicional de complejidad. A pesar de esto, navegar por este entorno dinámico ha sido una experiencia enriquecedora, impulsando mi capacidad para aprender y adaptarnos en un campo tecnológico en rápida evolución.
- **Experiencia con Reconocimiento Facial**: Por otro lado, trabajar con tecnología de reconocimiento facial ha sido fascinante. A diferencia de nuestra experiencia con blockchain, hemos encontrado un cúmulo de tutoriales y documentación sobre reconocimiento facial, lo que ha facilitado el proceso de aprendizaje y experimentación. Esta abundancia de recursos ha sido de mucho valor para el desarrollo eficiente y efectivo de nuestras soluciones basadas en IA.
- **Combinación de IA y Substrate**: Finalmente, hemos logrado crear un boceto de cómo combinar la inteligencia artificial y Substrate. Este proceso ha sido no solo técnicamente desafiante sino también increíblemente gratificante. La integración de estas dos tecnologías avanzadas ha abierto nuevas vías para soluciones innovadoras y ha demostrado ser un ejercicio estimulante en la resolución de problemas y la innovación tecnológica.

En resumen, aunque el proyecto presentó retos significativos, especialmente en términos de trabajar con tecnologías emergentes y en evolución como blockchain y Substrate, la experiencia ha sido extremadamente enriquecedora. He logrado no solo desarrollar habilidades técnicas avanzadas sino también una mejor comprensión de cómo las tecnologías emergentes pueden ser integradas para crear soluciones innovadoras.

6.2 Evaluación de Objetivos Planteados Inicialmente

Durante el desarrollo de este proyecto, he encontrado que el proceso ha sido más complicado y consumidor de tiempo de lo que inicialmente esperaba. Este desafío se ha presentado en varias etapas del desarrollo, afectando diversos aspectos del proyecto.

- **Construcción del Sistema**: La construcción del sistema en sí ha requerido una inversión significativa de tiempo y esfuerzo. La complejidad inherente a la implementación de una solución basada en blockchain,

combinada con la necesidad de integrar tecnologías avanzadas como el reconocimiento facial, ha resultado en un proceso de desarrollo más complejo de lo anticipado.

- **Desarrollo de un Pallet de Prueba de Existencia**: La creación de un pallet de prueba de existencia (proof of existence) en Substrate ha sido particularmente desafiante. A pesar de ser una funcionalidad aparentemente simple, su implementación ha requerido una comprensión profunda del framework de Substrate y Rust y una considerable inversión de tiempo para garantizar su correcto funcionamiento.
- **Llamadas RPC y Uso de IPFS**: Integrar llamadas RPC (Remote Procedure Call) y el intento de subir imágenes a la blockchain utilizando IPFS (InterPlanetary File System) ha agregado una capa adicional de complejidad. Estos elementos, aunque cruciales para la funcionalidad del sistema, han demandado un esfuerzo significativo para su correcta implementación y optimización.

Debido a estos desafíos, algunos aspectos del proyecto no se han podido llevar a cabo como se había planeado originalmente. En particular, los detalles finos relacionados con las restricciones, los accesos y el desarrollo de interfaces visuales más atractivas no se han podido refinar en la medida deseada. Si bien se ha logrado construir un sistema funcional que integra blockchain con tecnología de reconocimiento facial, el nivel de pulido y perfección en algunos aspectos del proyecto ha tenido que ser moderado debido a las limitaciones de tiempo y la complejidad encontrada durante el desarrollo.

Esta experiencia ha sido una lección importante en la gestión de expectativas y la planificación de proyectos que involucran tecnologías nuevas y en rápido desarrollo. A pesar de los obstáculos, los logros alcanzados proporcionan una base sólida sobre la cual se pueden realizar mejoras y refinamientos en el futuro.

6.3 Análisis de la Planificación y Metodología Seguida

En el transcurso del proyecto, he mantenido un seguimiento de la planificación inicial, aunque me he encontrado con la necesidad de dedicar más horas de lo previsto al desarrollo en blockchain.

- **Adaptación de la Planificación**: Aunque se ha seguido la planificación establecida, la inversión de tiempo adicional al desarrollo ha sido un factor crítico para garantizar la calidad y funcionalidad del sistema. Este esfuerzo extra se ha centrado especialmente en la parte de desarrollo en blockchain, donde las dificultades técnicas y las actualizaciones constantes del framework Substrate han requerido una atención y un tiempo mayores de lo anticipado.
- **Metodología Agile**: Desde el comienzo del proyecto, he adoptado una metodología Agile para el desarrollo. Esta metodología ha sido efectiva para adaptarse a los cambios y para manejar las incertidumbres inherentes al trabajar con tecnologías emergentes. La flexibilidad de Agile ha permitido ajustar el enfoque y las prioridades a medida que surgían nuevos desafíos y aprendizajes.
- **Necesidad de Retroalimentación Continua**: A pesar de que la estructura y el guion inicial podrían haber sugerido un enfoque más lineal o en cascada, la naturaleza del proyecto ha requerido una retroalimentación continua y ajustes en varios aspectos del desarrollo. Cada modificación, especialmente en el desarrollo del blockchain, ha

tenido impactos en otros componentes del proyecto, lo que ha hecho indispensable una revisión y adaptación constantes.

En conclusión, aunque la planificación inicial ha sido una guía útil, la naturaleza dinámica del desarrollo con tecnologías avanzadas y la propia complejidad del proyecto han requerido una adaptación continua y una inversión de tiempo adicional. La metodología Agile ha demostrado ser una elección acertada, proporcionando la flexibilidad necesaria para abordar los desafíos que surgieron y permitiendo una retroalimentación y ajustes continuos para asegurar el éxito del proyecto.

6.4 Evaluación de Impactos

El desarrollo de este proyecto ha estado relación con términos de sostenibilidad, ética social y diversidad. Estos aspectos son fundamentales para asegurar que la tecnología desarrollada no solo sea innovadora, sino también responsable y accesible.

- **Sostenibilidad**: Es importante reconocer que este proyecto, al ser intensivo en términos de uso de blockchain y procesamiento de reconocimiento facial, implica un mayor consumo de recursos y energía. La naturaleza 'pesada' del sistema, especialmente en términos de procesamiento y almacenamiento de datos, puede resultar en un mayor gasto de energía. Esto es una consideración importante desde el punto de vista de la sostenibilidad, y es un aspecto que podría ser abordado en futuros desarrollos para minimizar el impacto ambiental.
- **Aspectos Ético-Sociales**: A lo largo del desarrollo, se han respetado los aspectos éticos y sociales, asegurando que el sistema maneje los datos de forma segura y privada. Sin embargo, es crucial reconocer que el sistema actual no está implementado para ser accesible por personas con discapacidades visuales, lo cual podría interpretarse como una forma de discriminación. La accesibilidad es un componente esencial de la ética tecnológica y en este apartado se necesita mejora.
- **Diversidad**: La inclusión y la diversidad son aspectos críticos en el desarrollo de cualquier tecnología. En este proyecto, aunque no se ha implementado específicamente con un enfoque en la diversidad, es importante considerar cómo las futuras iteraciones pueden ser más inclusivas y accesibles para una gama más amplia de usuarios, incluyendo aquellos con diferentes capacidades y necesidades.

En resumen, mientras que el proyecto ha logrado avances significativos en términos de innovación tecnológica, hay áreas clave, especialmente en sostenibilidad y accesibilidad, que requieren una consideración y enfoque más profundos en el futuro. Abordar estos aspectos no solo mejorará la responsabilidad y el impacto social del proyecto, sino que también ampliará su aplicabilidad y accesibilidad a un público más diverso.

6.5 Trabajos Futuros

El desarrollo y la implementación de este proyecto han abierto varias vías para mejoras y expansiones futuras. A continuación, algunos aspectos que representan oportunidades para el desarrollo continuo:

1. **Mejorar el Reconocimiento Facial**: Aunque el sistema actual de reconocimiento facial es funcional, hay un amplio margen para su mejora. Esto incluye aumentar la precisión, la velocidad de procesamiento y la capacidad para funcionar en condiciones variadas de iluminación y con diferentes tipos de rostros. También es importante trabajar en la inclusión de características que aumenten la accesibilidad para usuarios con diversas capacidades.
2. **Hacer el Sistema Más Exigente y Verificable**: Es crucial mejorar la robustez del sistema en términos de seguridad y verificación. Esto incluye la implementación de procesos de verificación más estrictos, como la confirmación de email, la seguridad web avanzada y otras medidas de autenticación. Estas mejoras asegurarán que el sistema sea más resistente frente a intentos de acceso no autorizado y uso fraudulento.
3. **Añadir Almacenamiento de Imágenes con IPFS en Blockchain**: Una de las mejoras planificadas es la integración del almacenamiento de imágenes utilizando IPFS (InterPlanetary File System) en la blockchain. Esto no solo mejorará la eficiencia en el manejo de datos, sino que también aumentará la descentralización y la seguridad del almacenamiento de información, un aspecto crucial para sistemas basados en blockchain.
4. **Asegurar el Funcionamiento Óptimo de Blockchain Dentro del Sistema**: Es fundamental garantizar que la implementación de la blockchain funcione de manera óptima dentro del sistema. Esto implica una revisión continua y mejoras en la arquitectura blockchain, la optimización del rendimiento, la reducción del consumo de recursos y la mejora de la escalabilidad. Un funcionamiento eficiente de la blockchain es vital para la sostenibilidad general del sistema y su capacidad para manejar transacciones y datos a gran escala.

Estos trabajos futuros representan pasos esenciales hacia la mejora del sistema, asegurando que permanezca a la vanguardia de la tecnología. La implementación de estas mejoras no solo fortalecerá la funcionalidad del sistema, sino que también ampliará su aplicabilidad y relevancia en un mundo tecnológico en constante evolución.

7. Glosario

1. **Blockchain**: Tecnología de registro distribuido que mantiene una lista creciente de registros, llamados bloques, que están interconectados y asegurados mediante criptografía.
2. **Inteligencia Artificial (IA)**: Campo de la informática que se enfoca en crear sistemas capaces de realizar tareas que normalmente requieren inteligencia humana.
3. **FaceNet**: Un sistema de reconocimiento facial desarrollado por Google, que utiliza aprendizaje profundo para transformar imágenes faciales en vectores característicos en un espacio multidimensional.
4. **Substrate**: Framework de desarrollo de blockchain diseñado para ser flexible y abierto, permitiendo a los desarrolladores construir blockchains personalizadas.
5. **Identidad Digital**: Representación digital de una persona o entidad en la red, compuesta por un conjunto de atributos o credenciales digitales verificables.
6. **Parachains**: En el contexto de blockchain, son cadenas de bloques individuales que funcionan en paralelo dentro de un ecosistema más amplio, como la red Polkadot.
7. **GDPR**: Reglamento General de Protección de Datos, una regulación de la Unión Europea que establece normas sobre el manejo de datos personales.
8. **Triplet Loss**: Una función de pérdida utilizada en el aprendizaje profundo, especialmente en sistemas de reconocimiento facial, para diferenciar efectivamente entre diferentes caras.
9. **Smart Contracts**: Contratos autoejecutables almacenados en una blockchain, que se activan automáticamente cuando se cumplen condiciones predefinidas.
10. **DIDs (Identificadores Descentralizados)**: Identificadores únicos utilizados en blockchains para verificar la identidad de un individuo o entidad de manera segura y descentralizada.
11. **Reconocimiento Facial**: Tecnología que identifica o verifica una persona a partir de una imagen digital o un video.
12. **Aprendizaje Automático:** Subcampo de la inteligencia artificial que se enfoca en el desarrollo de sistemas que pueden aprender y mejorar a partir de la experiencia.
13. **WebAssembly:** Formato de código binario para ejecutables que permite la ejecución de código a nivel de máquina en un navegador web.
14. **EVM (Ethereum Virtual Machine**): Entorno de ejecución para smart contracts en la red Ethereum.
15. **NIST (Instituto Nacional de Estándares y Tecnología):** Agencia del Departamento de Comercio de EE. UU. que desarrolla tecnología, métricas y estándares.
16. **Biometría:** Método de identificación basado en características físicas o de comportamiento únicas de los individuos.
17. **Javascript:** Lenguaje de programación interpretado, comúnmente utilizado para scripts del lado del cliente en páginas web.
18. **CSS (Hojas de Estilo en Cascada):** Lenguaje de diseño gráfico para definir y crear la presentación de un documento estructurado escrito en HTML.
19. **Rust:** Lenguaje de programación centrado en la seguridad, la concurrencia y el rendimiento.

20. **API Polkadot JS:** Interfaz de programación de aplicaciones para interactuar con la red Polkadot.
21. **Identidad Autosoberana:** Modelo de identidad digital donde los usuarios tienen control total sobre sus propias identidades y datos.
22. **Cadena Génesis:** El primer bloque de una cadena de bloques, utilizado como punto de partida de la blockchain.
23. **Código Abierto:** Software cuyo código fuente es accesible al público para su uso y modificación.
24. **Interoperabilidad:** Capacidad de sistemas informáticos o software para intercambiar y hacer uso de información.
25. **Peer-to-Peer (P2P):** Red descentralizada donde cada participante (peer) actúa como cliente y servidor.
26. **Consensus Algorithm:** Proceso utilizado en una red de blockchain para lograr un acuerdo necesario en un estado de red único.
27. **Pallets en Substrate:** Módulos reutilizables que proporcionan funcionalidades específicas en el desarrollo de blockchains con Substrate.
28. **Credenciales Digitales:** Evidencia electrónica que certifica una afirmación o atributo de una entidad o individuo.
29. **Cifrado Criptográfico:** Uso de técnicas matemáticas para asegurar la información, haciendo que sea incomprensible sin una clave secreta, esencial en la seguridad de blockchain.
30. **Framework de Desarrollo:** Estructura conceptual y tecnológica utilizada como soporte para el desarrollo y organización de software.
31. **Red Polkadot:** Red blockchain que permite la transferencia de mensajes y valor entre cadenas de bloques diferentes, buscando interoperabilidad y escalabilidad.
32. **KYC (Conozca a Su Cliente):** Proceso utilizado por empresas para verificar la identidad de sus clientes.
33. **GDPR (Reglamento General de Protección de Datos):** Reglamento de la UE que establece directrices para la recopilación y procesamiento de datos personales de individuos dentro de la Unión Europea.

8. Bibliografía

[1] 14/10/2023: Why Traditional Identity Verification Methods Are On Their Way Out
[2] 14/10/2023: #CybersecurityAwarenessMonth - Multifactor Authentication (MFA): Enhancing Digital Security
[3] 14/10/2023: Biometric Authentication vs. Traditional Methods: Pros and Cons
[4] 14/10/2023: Biometrics vs. Traditional Authentication: A Comparative Analysis of Security Measures
[5] 14/10/2023: How effective are traditional authentication methods?
[6] 21/10/2023: Definición y concepto de Identidad | Conceptualia
[7] 21/10/2023: ¿Qué significa Identidad en Filosofía? | Mis Filosofías ®✔ (misfilosofias.com)
[8] 21/20/2023: Identidad (ciencias sociales) - Wikipedia, la enciclopedia libre
[9] 21/10/2023: Los Documentos Identificativos: el D.N.I. o el N.I.E.. Digitalización del DNI. (oficialdenotaria.com)
[10] 21/10/2023: La importancia de disponer del certificado digital - Infoautonomos
[11] 21/10/2023: ¿Qué es y por qué es importante la identidad digital? | BBVA
[12] 21/10/2023: Blockchain Para La Identidad Digital: La Identidad Descentralizada y Auto-Soberana (SSI) (https_101blockchains.com)
[13] 21/10:2023: Blockchain and biometrics
[14] 21/10/2023: La identidad digital 2.0 y las tecnologías que la hacen posible (vasscompany.com)
[15] 21/10/2023: Casos de Uso del Blockchain: Identidad Digital | Binance Academy
[16] 22/10/2023: (9) Identidad digital descentralizada | LinkedIn
[17] 22/10/2023: Identificadores Descentralizados: ya son Recomendación W3C – W3C Hispano
[18] 22/10/2023: Decentralized Identifiers (DIDs) v1.0 (w3.org)
[19] 22/10/2023: DID, la descentralización es clave en la nueva identidad digital | Didit
[20] 22/10/2023: Identidad Auto-Soberana y Zero Knowledge Proof - Extrimian
[21] 22/10/2023: Qué es la Auto-Identidad Soberana (SSI - Self-Sovereign Identity) - Resiliente Digital
[22] 28/10/2023 :https://www.thalesgroup.com/es/countries/americas/latin-america/dis/gobierno/inspiracion/historia-del-reconocimiento-facial
[23] 28/10/2023: https://www.tecalis.com/es/blog/reconocimiento-facial
[24] 28/10/2023: Face Detection and ResNet-50 | Kaggle
[25] 28/10/2023: GitHub - ox-vgg/vgg_face2
[26] 28/10/2023: GitHub - serengil/deepface
[27] 28/10/2023: GitHub - ashushekar/VGG16
[28] 28/10/2023: GitHub - timesler/facenet-pytorch
[29] 28/10/2023: FaceNet: uso del sistema de reconocimiento facial – Barcelona Geeks
[30] 28/10/2023: Introduction to FaceNet
[31] 28/10/2023: Introduction to the FaceNet Architecture · Syntric AI
[32] 29/10/2023: FaceNet Architecture. The comprehension in this article comes… | by Milind Deore | Analytics Vidhya | Medium
[33] 29/10/2023: neural networks - Detailed explaination of Facenet Model for face recogniton? - Artificial Intelligence Stack Exchange

[34] 29/10/2023: Reconocimiento Facial con Machine Learning: FaceNet y one-shot learning | Codificando Bits
[35] 29/10/2023: ¿Cómo crear un modelo de reconocimiento facial usando FaceNet Keras? (ichi.pro)
[36] 04/11/2023: Substrate Blockchain Technology | Substrate_
[37] 04/11/2023: Parity Substrate: How to Build a Blockchain in 15 Minutes | Apriorit
[38] 04/11/2023: Introductory Tutorial for Blockchain Developers
[39] 04/11/2023: Substrate: A Framework To Efficiently Build Different Blockchains
[40] 04/11/2023: Flexible Blockchain | Substrate
[41] 04/11/2023: Substrate Blockchains and Runtime Modules: An Introduction
[42] 04/11/2023: Smart Contracts | Substrate
[43] 04/11/2023: Prepare your first contract | Substrate Docs
[44] 04/11/2023: https://www.antiersolutions.com(www.antiersolutions.com)
[45] 04/11/2023: Substrate blockchain development: Core concepts - LogRocket Blog
[46] 04/11/2023: Interoperable Blockchain | Substrate
[47] 04/11/2023: Substrate Framework | For Efficient Blockchain Development
[48] 04/11/2023: Architecture and Rust libraries | Substrate_ Docs (main--substrate-docs.netlify.app)
[49] 04/11/2023: The Polkadot architecture and introduction to the Substrate infrastructure (cointelegraph.com)
[50] 05/11/2023: Parachains | Next-Generation Blockchains | Polkadot
[51] 05/11/2023: How to use Substrate to create Parachains in Polkadot (zeeve.io)