Sistema de almacenamiento distribuido de documentos basado en Blockchain

Curricular Tecnología en Sistematización de Datos de la Universidad Distrital Francisco José de Caldas



Ivan Ferney Rodriguez Rojas

Shanexon Steven Ortiz Ramírez

Universidad Distrital Francisco José de Caldas

Tecnología en Sistematización de Datos

Facultad Tecnológica

Bogotá D.C.

Sistema de almacenamiento distribuido de documentos basado en BlockChai

Curricular Tecnología en Sistematización de Datos de la Universidad Distrital Francisco José de Caldas

Ivan Ferney Rodriguez Rojas

Shanexon Steven Ortiz Ramírez

Proyecto de grado para optar al título de

Tecnología en Sistematización de Datos

Tutor: Luis Felipe Wanumen Silva

Universidad Distrital Francisco José de Caldas

Tecnología en Sistematización de Datos

Facultad Tecnológica

Agosto 2025

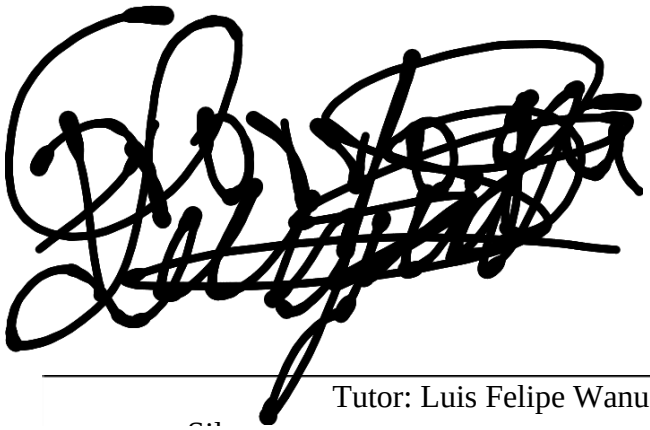
Nota de aceptación:

_____

_____

_____

_____



_____

Tutor: Luis Felipe Wanumen

_____

Jurado: Miguel Angel Leguizamón

Bogotá,

Agradecimientos

Quiero expresar mi sincero agradecimiento a mi familia, por su apoyo constante y motivación en cada etapa de este proceso; a mis profesores y tutores, quienes con sus orientaciones y conocimientos enriquecieron de manera invaluable la construcción de este trabajo; y a mis compañeros y amigos, que con sus ideas, compañía y palabras de ánimo hicieron más llevadero el camino hacia la culminación de esta investigación.

.

Resumen

Este trabajo aborda el problema de la falta de un sistema confiable para el almacenamiento y la consulta de certificados académicos internos en la Universidad Distrital Francisco José de Caldas, lo cual genera riesgos de manipulación, pérdida de información y demoras en los procesos administrativos.

El objetivo principal fue desarrollar un sistema de almacenamiento distribuido basado en tecnología blockchain e IPFS que permitiera garantizar la veracidad, integridad e inmutabilidad de los documentos académicos.

La metodología empleada fue de tipo experimental, mediante el diseño, desarrollo e implementación de un prototipo en un entorno local. Se construyó un contrato inteligente para el registro de documentos y una aplicación web que permite su carga, consulta y verificación.

Como resultado, se obtuvo un sistema funcional capaz de registrar y validar documentos en tiempos promedio inferiores a dos segundos por consulta, con una coincidencia del 100 % entre los identificadores almacenados y los documentos verificados. Estos resultados demuestran

la viabilidad técnica del uso de blockchain en la gestión documental académica.

El principal aporte del proyecto es la optimización de los procesos de almacenamiento y verificación de certificados, reduciendo los riesgos de fraude y mejorando la eficiencia administrativa. Esta solución beneficia directamente a estudiantes, egresados, empleadores y a la institución, fortaleciendo la confianza en los documentos emitidos.

.

Abstract

This project proposes the development of a system designed for the registration and verification of academic certificates using blockchain and IPFS technologies. Unlike traditional software that issues diplomas, this solution assumes that certificates are already generated by the university and focuses on recording a unique identifier—a hash—on the blockchain, which allows their authenticity to be verified at any time. The aim is to streamline validation processes,

strengthen protection against forgery, and provide graduates with a reliable tool to prove the legitimacy of their academic achievements.

The system combines an application layer capable of generating and managing these records, a blockchain network that guarantees the immutability of the information, and an integration layer through an API that connects to the user interface. This setup enables real-time verification whenever a certificate is presented, ensuring that it matches the document registered on the chain. By implementing this approach, the project seeks to modernize academic document management, reinforce trust in university-issued certificates, and position the institution as a leader in the adoption of innovative technologies within higher education.

Tabla de Contenido

Agradecimientos 1

Resumen 2

Abstract 3

Introducción 9

Planeación 10

1.1. Planteamiento del Problema 10

1.2. Justificación 11

1.3. Objetivos 13

1.3.1. Objetivo General 13

1.3.2. Objetivos Específicos 13

1.4. Alcance 14

1.5. Limitaciones 14

1.6. Marco de Referencia 15

1.6.1. Estado del Arte 15

1.6.2. Marco Teórico 16

1.6.3. Marco Metodológico 25

1.7. Factibilidad 28

1.7.1. Factibilidad Técnica 28

1.7.2. Factibilidad Operativa 29

1.7.3. Factibilidad Económica 29

1.7.4. Factibilidad Legal 31

1.8. Cronograma 32

Análisis 33

2.1. Análisis de Requerimientos 33

2.1.1. Requerimientos Funcionales 34

2.1.2. Requerimientos No Funcionales 35

2.1.3. Definición de actores 37

Diseño 39

3.1. Solución Tecnológica 39

3.1.2 Características del sistema 41

3.1.3. Herramientas de desarrollo utilizadas 42

3.2. Diagrama de Procesos 43

3.3. Diagrama de Arquitectura 46

3.3.2 **Capa de Lógica / Aplicación (Back-end / Smart Contracts)** 47

Implementación 50

4.1. Infraestructura local / Entorno de desarrollo 50

4.1.1. Estructura de carpetas 50

4.1.2. Blockchain local 52

4.1.3. IPFS local o en Pinata 52

4.2. Almacenamiento de documentos (IPFS) 53

4.2.1. Ejemplo práctico de CID 53

4.2.2. Consideraciones Finales 54

4.3. Aplicación / Lógica del sistema 54

4.3.1. Interfaz de Carga de Documentos 54

4.3.2. Búsqueda de documentos 56

4.3.3. Visualización y verificación de documentos 57

4.4. Smart Contracts / Blockchain 60

4.4.1. Código del contrato DocumentStorage.sol 60

4.4.2. Archivo de configuración truffle-config.js 63

4.5. Análisis de Riesgos y Situaciones 66

Anexo 2: Manual de Uso 69

5.1.2. Subir Documentos 69

Recomendaciones 75

Conclusiones 76

Bibliografía 78

Lista de Tablas

Tabla 1: Cuadro Comparativo Sistemas Tradicional de Autenticación 24
Tabla 2: Cuadro Comparativo no. 2 sistema Tradicional de Autenticación 24
Tabla 3: Actividades Metodología Scrum 27
Tabla 4: Factibilidad Económica - Mano de Obra 30
Tabla 5: Factibilidad Económica - Recursos Técnicos 30
Tabla 6: Factibilidad Económica - Costo Total 30
Tabla 7: Registro de Documentos 34
Tabla 8: Registro de Eventos 34
Tabla 9: Consulta de Documentos 35
Tabla 10: Disponibilidad y Rendimiento 36
Tabla 11: Escalabilidad 36
Tabla 12: Integridad de Datos 36

Tabla 13: Actor - Administrador 37
Tabla 14:Actor - Estudiante 37
Tabla 15:Análisis de Riesgos y Estrategias de Mitigación 67

Lista de Ilustraciones

Ilustración 1:Cronograma 33
Ilustración 2: Representación Flujo - Grafico 44
Ilustración 3: Diagrama de Flujo Sistema de Gestión de Documentos Blockchain 46
Ilustración 4: Diagrama de Arquitectura 47
Ilustración 5: Estructura Carpetas 52
Ilustración 6: Generar IPFS 54
Ilustración 7: Interfaz Carga de Documentos 56
Ilustración 8: Interfaz Búsqueda de Documentos 58
Ilustración 9: Visual Verificación de Documentos 59
Ilustración 10: Visual Botones Principales 70
Ilustración 11: Componente Visual Cargar un Documento 71
Ilustración 12: Visualización Documentos Cargados 72

Ilustración 13: Visual Busqueda de Documento 74
Ilustración 14: CODIGO QR - ID DOCUMENTO 75

Introducción

En la actualidad, los documentos académicos representan un elemento fundamental en la vida profesional y académica de los estudiantes, ya que certifican formalmente sus competencias y logros. Sin embargo, los procesos tradicionales para su almacenamiento, consulta y verificación presentan limitaciones relacionadas con tiempos prolongados, riesgos de manipulación y dependencia de sistemas centralizados.

En la Universidad Distrital Francisco José de Caldas, la gestión de certificados internos continúa realizándose mediante procedimientos manuales o plataformas centralizadas, lo cual incrementa la carga administrativa y expone la información a posibles alteraciones o pérdidas. Esta situación evidencia la necesidad de implementar soluciones tecnológicas que garanticen mayor seguridad, integridad y disponibilidad de los documentos.

En este contexto, el presente trabajo propone el desarrollo de un sistema de almacenamiento distribuido de documentos basado en tecnología blockchain e IPFS, con el fin de asegurar que los

certificados académicos puedan ser almacenados, consultados y verificados de manera confiable e inmutable.

El cumplimiento de los objetivos planteados se presenta a lo largo del documento de la siguiente manera: en el primer capítulo se aborda el planteamiento del problema, la justificación y los objetivos; en el segundo capítulo se desarrolla el análisis de requerimientos; en el tercer capítulo se presenta el diseño del sistema; en el cuarto capítulo se describe la implementación del prototipo; y finalmente, en el quinto capítulo se exponen los resultados, conclusiones y recomendaciones.

De esta forma, el trabajo integra aspectos teóricos y prácticos que permiten demostrar la viabilidad técnica del uso de blockchain como herramienta para la gestión segura de documentos académicos.

Con esto en mente, el presente trabajo se enfoca en diseñar y desarrollar un prototipo apoyado en tecnologías de registro inmutable. El cumplimiento de los objetivos propuestos se presenta a lo largo del documento de la siguiente manera:

- **Fundamentación y Requerimientos:** En el **Capítulo 2** se cumple el primer objetivo mediante el levantamiento de información técnica y la definición de la arquitectura necesaria red, software y hardware para que la solución funcione.
- **Marco Tecnológico:** El **Capítulo 3** aborda el segundo objetivo y se sumerge en el funcionamiento de Blockchain y del almacenamiento descentralizado IPFS, analizando con ejemplos y comparaciones las ventajas de seguridad frente al sistema actual.
- **Desarrollo del Prototipo:** En el **Capítulo 4** se aplican principios de ingeniería para construir la herramienta, integrando contratos inteligentes que permiten la carga y el registro inalterable de certificados (**Objetivo 3**).
- **Validación y Resultados:** Finalmente, en el **Capítulo 5** se demuestra la integración de la red Blockchain con un caso de uso real de la Universidad Distrital, evaluando la utilidad de la tecnología en procesos académicos y administrativos (**Objetivo 4**).

Cabe precisar que la interacción con Blockchain e IPFS en este trabajo se realiza de manera

simulada con fines académicos, enfocándose en demostrar técnicamente el prototipo y su capacidad de consulta verídica ante el ente regulador.

Capítulo 1

Planeación

1.1. Planteamiento del Problema

En la Universidad Distrital, el proceso para que un egresado obtenga y valide su certificado académico presenta limitaciones que afectan tanto a los estudiantes como a terceros que requieren verificar la autenticidad de estos documentos. Actualmente, la validación depende de procedimientos manuales realizados por el personal administrativo y puede tardar entre cinco y quince días hábiles. Este tiempo de espera representa una barrera significativa, especialmente en situaciones que requieren una respuesta rápida, como postulaciones laborales o admisiones académicas.

Además, aunque el formato digital ha facilitado la entrega de certificados, no ha eliminado los riesgos asociados a la falsificación, alteración o manipulación de la información. Este tipo de vulnerabilidades compromete la confianza en la validez de los documentos y puede afectar la reputación de la institución. La ausencia de un sistema de verificación inmediata también genera cargas administrativas innecesarias y limita la capacidad de respuesta frente a solicitudes externas.

En otros contextos, la tecnología blockchain ha demostrado ser efectiva para garantizar la integridad y autenticidad de información sensible. Países como Ghana, Kenia y Nigeria la han implementado para registrar títulos de propiedad, evitando fraudes y pérdidas de documentos, y en otros casos, se ha utilizado para asegurar procesos electorales mediante voto electrónico. Estos antecedentes evidencian su potencial para crear registros inmutables y verificables desde cualquier lugar, lo que la hace una alternativa viable para modernizar la gestión de certificados académicos.

Este proyecto propone desarrollar una herramienta que use **blockchain** para registrar la huella digital (hash) de cada certificado académico emitido por la Universidad Distrital e **IPFS** para su almacenamiento descentralizado, garantizando integridad, disponibilidad y reduciendo la dependencia de servidores únicos. Con ello, terceros podrán verificar su autenticidad de forma inmediata, mejorando la seguridad, acortando los tiempos de validación y optimizando la gestión. La pregunta central es: **¿puede un sistema basado en blockchain e IPFS asegurar la verificación inmediata y confiable de los certificados académicos de la Universidad Distrital, evitando fraudes y demoras?**

1.2. Justificación

En el mundo académico, un certificado universitario no es simplemente un papel o un archivo digital: representa años de estudio, esfuerzo y dedicación. Sin embargo, en la práctica, validarlo no siempre resulta tan ágil como debería. En la Universidad Distrital Francisco José de

Caldas, por ejemplo, la verificación de un documento puede tardar varios días, incluso semanas, dependiendo de la carga administrativa y de la complejidad del caso. Para un egresado que busca empleo o necesita presentar su certificado para continuar con sus estudios, esa espera puede significar la pérdida de una oportunidad valiosa.

El problema va más allá del tiempo. Aunque los documentos digitales facilitan su gestión, también son vulnerables a la manipulación. No es imposible —y de hecho ocurre— que un certificado sea falsificado o alterado, lo que afecta la confianza en la institución y complica los procesos de validación. Situaciones similares han sido observadas en otros contextos: en Ghana, por ejemplo, la iniciativa Bitland buscó implementar blockchain para registrar títulos de propiedad y prevenir tanto la corrupción como la pérdida de documentos. Su objetivo era generar registros inalterables y accesibles, aunque diversos estudios señalan que enfrentó importantes desafíos técnicos y legales que limitaron su alcance. [1] En Kenia y Nigeria también se han desarrollado proyectos basados en blockchain con la intención de reducir el fraude y aumentar la transparencia en registros oficiales. [2]

La tecnología blockchain, ampliamente reconocida por su papel en las criptomonedas, ofrece mucho más que un sistema financiero descentralizado. Sus propiedades de inmutabilidad, transparencia y seguridad criptográfica han demostrado ser valiosas en campos como la gestión de tierras o el voto electrónico. Porxas y Conejero destacan, por ejemplo, su potencial para crear registros digitales confiables y anónimos en sistemas de votación, donde la seguridad y la veracidad del registro son esenciales [3]. Si blockchain puede proteger un voto, ¿por qué no podría proteger un título universitario?

Con este proyecto se busca aplicar blockchain en conjunto con IPFS (Sistema de Archivos Interplanetario) para que los certificados académicos emitidos previamente por la universidad puedan **subirse y registrarse** en una red descentralizada, quedando asociados a un identificador único (hash) que facilita su verificación posterior. De esta manera, los tiempos de validación pasarían de días a segundos y los egresados contarían con un sistema moderno, confiable y accesible para acreditar sus logros. Al mismo tiempo, la Universidad Distrital tendría

la oportunidad de posicionarse como pionera en Colombia en la adopción de tecnologías emergentes aplicadas a la gestión académica, fortaleciendo su imagen institucional y generando beneficios concretos para estudiantes, empleadores y aliados académicos.

1.3. Objetivos

1.3.1. Objetivo General

El objetivo general es requiere un software o una herramienta tecnológica que me permita almacenar y consultar mis certificados internos emitidos por un ente regulatorio en este caso la Universidad Distrital, el cual se encargará de constatar que este documento sea verídico ante tal ente, puesto que de una o otra forma su registro no podrá ser alterado

1.3.2. Objetivos Específicos

- A partir de un relevamiento del tema de trabajo elegido y del material disponible en fuentes primarias y secundarias, se decide la estructura de la red y el software y hardware necesario.
- Conozca cómo funciona blockchain y la tecnología debido a su reciente auge masivo y las amplias posibilidades que ofrece.
- Aplicar y profundizar los conocimientos aprendidos y las técnicas utilizadas durante la carrera, todo lo cual contribuye en gran medida al desarrollo general del trabajo.
- La integración de redes blockchain con casos de uso del mundo real para demostrar la utilidad de la tecnología en el mundo empresarial.

1.4. Alcance

La meta principal de este trabajo es dar vida a un prototipo funcional de un sistema web local para gestionar documentos académicos. La verdad es que no buscamos solo "hacer una

página", sino crear un caso de estudio real que nos permita poner a prueba si la tecnología Blockchain es tan revolucionaria como dicen para nuestra universidad.

Para lograrlo, nos hemos propuesto un camino claro:

- **Sumergirnos en la tecnología:** Primero, nos dedicaremos a investigar y elegir con pinzas la infraestructura ideal. Vamos a configurar todo el software necesario —desde React hasta Solidity e IPFS— basándonos en lo que encontremos en las fuentes más confiables. Y es que, al final del día, una buena base técnica es lo que sostiene cualquier gran idea.
- **Cuidar la integridad de los documentos:** Queremos que el proceso sea sencillo pero robusto. Cuando un estudiante suba un archivo (ya sea un PDF de su título o una foto en PNG/JPG), el sistema se encargará de crear un "hash" único. Este código es como una huella digital que se registra en un Smart Contract; así, nos aseguramos de que el documento sea inalterable y de que nadie pueda meterle mano después
- **Verificar sin intermediarios:** Además, diseñaremos un módulo de consulta pública. La idea es que cualquiera pueda localizar un documento simplemente con el número de identificación. El sistema no solo mostrará el archivo en IPFS, sino que permitirá validar su autenticidad mediante códigos QR, casi como si estuviéramos auditando la información en tiempo real.
- **Interfaz sencilla:** navegación básica para subir y buscar documentos, con diseño responsivo y amigable.
- **Aprender en el laboratorio:** Por último, pondremos todo a prueba en un entorno controlado (una testnet). Siendo sinceros, no pretendemos que esto salga a producción mañana mismo; lo que realmente nos mueve es demostrar que este flujo es viable y que puede ahorrarle muchos dolores de cabeza y costos a la institución en el futuro.

El alcance se limita a pruebas locales, sin autenticación avanzada ni seguridad de producción, priorizando la validación del flujo y la viabilidad técnica.

1.5. Limitaciones

El sistema propuesto se desarrollará únicamente en un entorno local, sin conexión a redes públicas y utilizando datos ficticios. Estará enfocado en la gestión de documentos académicos en formatos PDF, PNG y JPG, sin contemplar otros tipos de archivo ni grandes volúmenes de información.

La interacción con blockchain e IPFS será simulada, evitando costos reales y limitándose a fines académicos. El proyecto no abordará aspectos legales o normativos, ya que su alcance se centra en la demostración técnica y conceptual del prototipo.

1.6. Marco de Referencia

1.6.1. Estado del Arte

En Colombia, el uso de blockchain en el ámbito académico ya no es una promesa lejana, sino una realidad. Instituciones como la Universidad EAN y la Universidad Nacional de Colombia han comenzado a emitir diplomas digitales certificados en blockchain, lo que les permite ofrecer a sus egresados documentos fáciles de verificar y prácticamente imposibles de falsificar. Estas experiencias demuestran que la tecnología no solo es viable, sino que también responde a necesidades reales del sector educativo.

Por ejemplo, la **Universidad EAN** se convirtió en la primera universidad del país en emitir títulos certificados en blockchain, gracias a un convenio con el Título, desarrollado por Thomas Signe. Desde 2019 sus graduandos obtienen diplomas digitales inviolables, con validez legal, fáciles de compartir y verificar en redes sociales o plataformas de recursos humanos [4] [5]. Más que un flash tecnológico, es una transformación real: los egresados ya no tienen que esperar ni depender de papeleo.

Apenas unos meses después, en mayo de 2019, la **Universidad Nacional de Colombia (UNAL)** también ingresó a esta era. Empezó a emitir Títulos (títulos electrónicos) con blockchain, que incluyen firma digital, sello de tiempo y se pueden verificar en línea con un código QR o hash. Lo curioso es que inicialmente lo probaron con estudiantes de educación continua y luego escalaron la idea para todos sus graduados [6]. Así, ya no hacen falta llamadas ni correos interminables para confirmar un diploma.

La realidad va más allá de dos universidades de élite. Otras como la **Universidad de Córdoba**, que lleva títulos digitales en blockchain a la región Caribe, o instituciones como

Sanitas, Libre, Konrad Lorenz, Autónoma de Occidente y CEAD, entre otras, están adoptando la tecnología de eTítulo para certificar títulos y diplomas [5]. Un mosaico interesante —cada institución con sus ventajas específicas, pero todas con un objetivo claro: seguridad, trazabilidad y menos burocracia.

- **Viabilidad tecnofuncional**: la EAN y la UNAL demostraron que integrar blockchain en los certificados académicos no es un experimento de laboratorio, sino una solución operativa.

- **Adopción creciente**: más universidades lo implementan en el país, lo que permite ver el camino y, sobre todo, aprender de los retos técnicos y de integración que enfrentaron.

- **Espacio para aportar**: aunque hay avances, todavía faltan desarrollos que cubran aspectos como privacidad, acceso descentralizado (por ejemplo, con IPFS), interoperabilidad real y facilidad de verificación al estilo "un clic" desde una convocatoria laboral o un sistema externo.

Aunque los avances son importantes, aún existen vacíos en temas de privacidad, almacenamiento descentralizado y usabilidad. Es justamente en ese espacio donde se ubica este proyecto, buscando aportar una solución adaptada al contexto de la Universidad Distrital Francisco José de Caldas.

1.6.2. Marco Teórico

En el corazón del problema están tres ideas simples, pero potentes: **integridad** (que el documento no cambie), **autenticidad** (que venga de quien dice venir) y **no repudio** (que nadie pueda negar su autoría). En términos técnicos, esto se apoya en funciones **hash** (como SHA-256) y en **firmas digitales**—mecanismos estandarizados que la comunidad técnica y regulatoria lleva años usando. El estándar de NIST para *hashes* (FIPS 180-4) describe cómo una mínima alteración en un archivo cambia por completo su "huella" digital; eso es justo lo que nos interesa

para detectar manipulaciones. Por su parte, el estándar de firmas digitales (FIPS 186-5) sienta las bases para verificar con criptografía pública que algo fue firmado por una entidad específica. [7]

En Colombia, además, existe un marco jurídico que reconoce la validez de los **mensajes de datos** y la **firma digital/electrónica**—piedra angular para que un certificado electrónico tenga efectos reales. La **Ley 527 de 1999** reguló el tema y abrió camino a la contratación y la prueba electrónica; más tarde el **Decreto 2364 de 2012** desarrolló la firma electrónica, útil para escenarios donde se requiere trazabilidad y verificación. [8] En un proyecto universitario, estas normas funcionan como "piso" legal para diseñar un flujo de emisión y verificación que sea aceptable ante terceros.

Blockchain

Un libro contable compartido. Cada "página" (bloque) encadena a la anterior con *hashes* y, dentro, las transacciones se agrupan usando **árboles de Merkle**, lo que permite verificar rápidamente si un dato pertenece al conjunto sin revelar todo el contenido. La propuesta original de [9] resolvió cómo acordar ese libro en redes abiertas con **prueba de trabajo**; después llegaron variantes con otros consensos. [9] Para una visión didáctica y completa, el libro de Narayanan et al. explica a fondo estas piezas: bloque, cadena, Merkle, consenso y ataques típicos. [10]

La forma de "ponerse de acuerdo" (consenso) varía. En redes públicas se usa PoW o PoS; en entornos institucionales—como una universidad, donde hay participantes identificados—tiene sentido una **red permisionada**. **Hyperledger Fabric** es un ejemplo: separa *endorsement*, *ordering* y *validation*, permite políticas de endoso (p.ej., "m de n firmas") y módulos enchufables de consenso. Esa modularidad ayuda a cumplir requisitos de privacidad y rendimiento propios del sector educativo. [11]

Contratos Inteligentes y Redes Permisionadas

Smart Contac

Un **contrato inteligente** es código que ejecuta reglas del negocio en la cadena. En proyectos de certificación académica, el *smart contract* suele: (i) registrar la **huella (hash)** del documento, (ii) asociarla a metadatos (programa, fecha, emisor), y (iii) exponer funciones de **verificación**. Fabric, por ejemplo, ejecuta *chaincode* bajo políticas de endoso entre organizaciones (facultades, secretarías, oficinas) para que una transacción solo sea válida si las firmas requeridas están presentes. Esto brinda gobernanza y control fino sobre quién puede escribir o validar registros. [12] [13]

Aunque los *smart contracts* no sustituyen la ley, la literatura jurídica los viene analizando como acuerdos auto-ejecutables que se integran con el marco de firmas y evidencias electrónicas—útil para comprender alcances y límites en contextos universitarios y públicos. [14]

IPFS y direccionamiento por contenido

Guardar documentos completos **dentro** de la cadena no es eficiente ni recomendable por privacidad. Por eso se usa **IPFS**, un sistema distribuido que **direcciona por contenido**: el identificador (*CID*) de un archivo depende de su *hash*. Si el archivo cambia, el CID cambia. Esto facilita comprobar integridad y distribuir copias sin depender de un único servidor. El artículo fundacional de Benet detalla cómo IPFS combina DHT, intercambio de bloques y verificación por *hash* para disponibilidad y eficiencia. En conjunto, *Blockchain + IPFS* permite registrar en cadena solo la huella y mantener el binario fuera, con control del acceso. [15]

Identidad descentralizada y credenciales verificables

Para que la verificación sea amigable (y no solo técnica), hoy se usan estándares W3C de **Decentralized Identifiers (DID)** y **Verifiable Credentials (VC)**. Un DID identifica de forma criptográfica a la entidad emisora (por ejemplo, la universidad) y una VC encapsula la afirmación "Este estudiante obtuvo tal título". Lo importante: un tercero puede **verificar** la firma de la credencial contra la clave pública del emisor, sin llamar a la universidad ni depender de su base

de datos en línea. El modelo 2.0 de *Verifiable Credentials* y la especificación de **DID Core** describen estos flujos y sus consideraciones de privacidad. [16]

Descentralización

La descentralización en blockchain implica la distribución del control y la toma de decisiones entre todos los participantes de la red, eliminando la necesidad de una autoridad central [17]. Cada nodo mantiene una copia del libro mayor y valida las transacciones de manera independiente, lo que incrementa la resistencia a fallos y ataques. Este enfoque es esencial para garantizar la autonomía y la seguridad en sistemas de autenticación de documentos universitarios, donde la integridad y la disponibilidad de la información son críticas. [18]

Inmutabilidad

Se refiere a la característica de que una vez que una transacción es registrada, no puede ser alterada ni eliminada. [19] Esto se logra mediante el uso de funciones criptográficas que enlazan cada bloque con el anterior, formando una cadena segura. En el contexto de la autenticación de documentos universitarios, esta propiedad asegura que los registros académicos no puedan ser modificados sin dejar evidencia, proporcionando un historial confiable y verificable. [20]

Transparencia

Las transacciones son visibles para todos los participantes de la red, aunque la identidad de los usuarios puede ser seudónima. Esta característica permite una auditoría pública y facilita la verificación de la autenticidad de los documentos. En el ámbito académico, esto permite a estudiantes, instituciones y empleadores verificar la validez de los títulos y credenciales de manera abierta y confiable. [21]

Seguridad

La seguridad en blockchain se logra mediante el uso de criptografía avanzada y mecanismos de consenso que garantizan la integridad y autenticidad de los datos. Estos mecanismos protegen la red contra fraudes y ataques, asegurando que solo las transacciones

válidas sean registradas. Para la autenticación de documentos universitarios, esto significa que los registros académicos están protegidos contra alteraciones no autorizadas y accesibles solo para partes legítimas. [22]

Consenso

El consenso en blockchain es el proceso mediante el cual todos los nodos de la red acuerdan la validez de las transacciones antes de que se añadan al libro mayor. Este acuerdo se logra mediante algoritmos como Prueba de Trabajo (PoW) o Prueba de Participación (PoS), que aseguran que todas las partes estén de acuerdo sobre el estado de la cadena. En la autenticación de documentos universitarios, un mecanismo de consenso confiable garantiza que solo los registros válidos sean aceptados y almacenados en la blockchain. [23]

Programabilidad

Como se mencionó anteriormente los contratos inteligentes son programas autoejecutables almacenados en la blockchain que automatizan acuerdos y procesos cuando se cumplen condiciones predefinidas. En el contexto de la autenticación de documentos universitarios, los contratos inteligentes pueden automatizar la emisión de certificados, validación de credenciales y otros procesos administrativos, reduciendo la necesidad de intermediarios y aumentando la eficiencia. [24]

Evidencia en educación superior: tendencias y casos

La literatura académica de los últimos años muestra un crecimiento sostenido de aplicaciones de blockchain en **diplomas, certificados y acreditación**. Existen revisiones sistemáticas que mapean beneficios (inmutabilidad, verificación sin intermediarios), retos (privacidad, escalabilidad, gobernanza) y brechas (usabilidad, adopción institucional). También hay estudios de caso recientes—por ejemplo, una plataforma nacional para **validación y equivalencias** de certificaciones en Emiratos Árabes—que reportan métricas de desempeño y decisiones de arquitectura transferibles a contextos universitarios. [25]

Más allá de la academia, gobiernos han probado blockchain en **registros de propiedad** (como Georgia, con su agencia de registro NAPR) y en **votación electrónica** con diferentes alcances, motivados por la trazabilidad y la auditoría independiente [26]. Estos casos, aunque de dominios distintos, sirven como analogía: si puedo verificar una escritura o un voto con garantías criptográficas y auditabilidad pública, también puedo verificar un **certificado universitario** sin depender de un correo o sello manual.

Escalabilidad

La capacidad de una red para manejar un número creciente de transacciones y usuarios sin comprometer su rendimiento, seguridad o descentralización. Es esencial para aplicaciones que requieren alta disponibilidad y eficiencia. [27]

Importancia en la autenticación de documentos: Una red blockchain escalable puede procesar múltiples solicitudes de verificación de documentos simultáneamente, garantizando tiempos de respuesta rápidos y evitando cuellos de botella. [27]

Mecanismos de Consenso en Blockchain

La Prueba de Trabajo es el mecanismo de consenso original utilizado por Bitcoin. En este sistema, los participantes (mineros) deben resolver complejos problemas matemáticos para validar las transacciones y añadir nuevos bloques a la cadena. Este proceso requiere una considerable cantidad de energía computacional, lo que puede generar preocupaciones medioambientales. Sin embargo, PoW ha demostrado ser efectivo en la prevención de ataques y en la protección de la red.

Prueba de Trabajo (Proof of Work - PoW): Una red blockchain escalable puede procesar múltiples solicitudes de verificación de documentos simultáneamente, garantizando tiempos de respuesta rápidos y evitando cuellos de botella. [29]

Prueba de Participación (Proof of Stake - PoS): La Prueba de Participación es una alternativa más eficiente en términos energéticos. En PoS, los validadores son seleccionados en función de la cantidad de criptomonedas que están dispuestos a "apostar" o bloquear como garantía. [30] Este enfoque reduce significativamente el consumo de energía y permite una

mayor escalabilidad. Ethereum, por ejemplo, implementó PoS para mejorar la eficiencia de su red.

Prueba de Autoridad (Proof of Authority - PoA): La Prueba de Autoridad es un mecanismo de consenso basado en la identidad y reputación de los validadores. En este sistema, los validadores son entidades conocidas y confiables, lo que permite una validación rápida y eficiente de las transacciones. PoA es comúnmente utilizado en redes privadas o consorciadas, donde la confianza en los participantes es esencia. [31].

Tokenización de Activos

La tokenización es el proceso de convertir activos físicos o digitales en tokens digitales que pueden ser gestionados en una blockchain. Esta práctica permite representar la propiedad de un activo de manera digital, facilitando su transferencia y división [28]. En el contexto académico, la tokenización puede aplicarse a títulos universitarios, creando representaciones digitales de los mismos que pueden ser fácilmente verificadas y transferidas.

Interoperabilidad entre Blockchains

La interoperabilidad se refiere a la capacidad de diferentes blockchains para comunicarse y compartir información entre sí. Esta característica es crucial para aplicaciones que requieren la integración de múltiples redes. En el caso de la autenticación de documentos universitarios, la interoperabilidad permitiría que títulos emitidos en diferentes universidades o países sean verificables a través de una plataforma común, facilitando su validación global.

Problemáticas en la Gestión Documental de la Universidad Distrital Francisco José de Caldas

La Universidad Distrital Francisco José de Caldas, como muchas instituciones de educación superior en Colombia, enfrenta retos importantes en la gestión de sus documentos. No es que no exista voluntad; de hecho, la universidad ha implementado programas de gestión documental, pero en la práctica se han encontrado con dificultades que ralentizan los procesos. Por ejemplo, en 2018 se reportó que la aplicación de instrumentos archivísticos adecuados era limitada, lo que generaba retrasos en la tramitación de documentos y complicaciones en los

procesos legales y administrativos [32]. Esto significa que incluso documentos importantes, como actas, certificados o resoluciones, podían tardar más de lo esperado en ser validados o entregados. Además, el personal a veces no contaba con la capacitación suficiente para manejar correctamente los sistemas documentales existentes, y los recursos tecnológicos eran limitados. Es decir, aunque se tengan las herramientas, si no hay entrenamiento ni infraestructura adecuada, los errores y retrasos son casi inevitables. [33]

En términos sencillos, podemos imaginarnos la universidad como un gran archivo lleno de documentos importantes, pero con muchos pasillos desordenados y algunas cerraduras difíciles de abrir. La gestión documental se convierte entonces en un desafío diario que afecta tanto a estudiantes como a funcionarios, y que requiere soluciones más innovadoras que las que los métodos tradicionales pueden ofrecer.

Desafíos en la Autenticación de Documentos Académicos

Otro punto crítico es la autenticación de documentos académicos. Sí, hablamos de certificados de notas, diplomas y otros documentos que necesitan ser confiables y verificables. Tradicionalmente, estos procesos dependen de sellos físicos, firmas manuales o registros en bases de datos internas. Pero, seamos sinceros, todos sabemos que los documentos pueden ser falsificados o manipulados, y aquí es donde surgen los problemas.

Un estudio reciente realizado en la universidad destacó que el uso de tecnologías tradicionales para la certificación digital aún es vulnerable a fraudes y errores humanos [34]. Piensa en la situación: un estudiante necesita enviar su diploma a otra institución o a un empleador, y si hay cualquier duda sobre la autenticidad del documento, el proceso se retrasa, genera estrés y, en el peor de los casos, puede afectar oportunidades laborales o académicas. En otras palabras, la universidad tiene documentos muy valiosos, pero los métodos tradicionales no siempre garantizan seguridad total.

Necesidad de Transformación Digital

Y bueno, como no podía ser de otra manera, la universidad ha empezado a reconocer que la transformación digital no es solo una tendencia, sino una necesidad real. Los sistemas actuales,

aunque funcionales en muchos aspectos, no logran ofrecer la rapidez, seguridad y transparencia que demanda la era digital. De hecho, proyectos apoyados por MinTIC y el PNUD han explorado el uso de blockchain para asegurar la integridad de diplomas y certificados académicos [35]. La idea es sencilla: ¿por qué no aprovechar una tecnología que permita que los documentos sean verificables en tiempo real y que nadie pueda alterarlos sin dejar rastro? Esta necesidad de modernización abre un espacio ideal para soluciones innovadoras como tu proyecto.

A continuación, se presentan cuadros comparativos que ilustran las diferencias entre los sistemas tradicionales de autenticación de documentos y tu propuesta basada en blockchain:

Tabla 1: Cuadro Comparativo Sistemas Tradicional de Autenticación

Característica	**Sistema Tradicional**	**Sistema Blockchain Propuesto**
Seguridad	Vulnerable a fraudes y alteraciones	Alta seguridad mediante inmutabilidad
Verificación	Requiere contacto directo con la universidad	Verificación instantánea en línea
Costos Operativos	Altos costos administrativos	Reducción de costos a largo plazo
Cumplimiento Legal	Cumple parcialmente con normativas	Cumple plenamente con normativas
Transparencia	Limitada y centralizada	Total transparencia y descentralización

Tabla 2: Cuadro Comparativo no. 2 sistema Tradicional de Autenticación

Proceso	Sistema Tradicional	Sistema Blockchain Propuesto
Emisión de Documentos	Manual y propenso a errores	Automática y precisa
Almacenamiento	Físico o en servidores locales	Descentralizado y seguro
Acceso a Información	Limitado y burocrático	Acceso libre y rápido
Auditoría	Compleja y costosa	Sencilla y transparente
Adaptabilidad Tecnológica	Baja	Alta, con integración a nuevas tecnologías

1.6.3. Marco Metodológico

El presente proyecto se desarrolló bajo un enfoque **experimental y de desarrollo de software**, ya que la finalidad principal fue implementar una solución tecnológica concreta que permita la autenticación de documentos universitarios mediante tecnología blockchain. La elección de este enfoque surge de la necesidad de **probar y validar conceptos**, en este caso, la descentralización, la inmutabilidad y la seguridad que ofrece la blockchain, dentro de un entorno controlado y seguro.

Se optó por un **entorno local** para la ejecución de todo el proyecto, lo que permitió un control total sobre las variables del sistema y una mayor libertad para experimentar sin depender de servicios externos. Esta decisión, además de garantizar la confidencialidad de los datos de prueba, facilitó la iteración rápida entre diseño, desarrollo y pruebas. Aunque podría parecer más

restrictivo que trabajar en la nube, en realidad permitió **un aprendizaje más profundo y directo**, donde cada error o fallo se podía analizar y corregir de inmediato.

Población y muestra

Dado que el proyecto es tecnológico y no se trabajó con personas reales ni datos externos, la **población de estudio** se define como el conjunto de documentos universitarios simulados y los nodos de la red blockchain local creados para las pruebas. La "muestra" la constituyen los **registros de prueba** generados para validar la autenticidad, la inmutabilidad y la eficiencia de la cadena de bloques. Por ejemplo, se crearon certificados de prueba con nombres y títulos ficticios, que luego se registraron en la blockchain local para verificar si el sistema podía autenticar cada uno de ellos correctamente, sin posibilidad de alteración.

Diseño del Sistema

Arquitectura del Sistema

Diseñar un backend con **Solidity**, utilizando un contrato inteligente llamado DocumentStorage, que **permitirá** registrar documentos asociados a cada usuario mediante su hash de IPFS y un timestamp, asegurando que cada registro sea único e inmutable.

Diseño de Base de Datos

Estructurar un sistema de almacenamiento local que **registrará** los hashes de los documentos junto con metadatos esenciales (fecha, tipo de documento, autor). La estructura **permitirá** crear un historial confiable de documentos sin necesidad de almacenamiento centralizado.

Diseño de Interfaces de Usuario

Desarrollar un frontend en **React**, que **proporcionará** una interfaz amigable para que los usuarios **puedan** subir documentos y verificar su autenticidad de manera directa. Por ejemplo, un estudiante **podrá** subir su diploma simulado y luego **consultar** si efectivamente **quedó registrado** en la blockchain, obteniendo una respuesta inmediata.

Desarrollo del Sistema

Subsistema de registro de documentos

Implementar una función, que **valide** que el hash tenga la longitud correcta de IPFS y lo **registrará** en la blockchain local. Cada acción **generará** un evento, lo que **permitirá** rastrear todas las operaciones realizadas por el usuario. Por ejemplo, cuando un usuario **suba** su certificado, se **emitirá** un evento con la fecha y la dirección del remitente.

Subsistema de Verificación

Crear una función, que solo pueda ser ejecutada por el propietario del contrato, demostrando cómo se controlarán las acciones administrativas dentro de la blockchain y evitando que cualquier usuario eliminen registros de otros**.**

Pruebas y Validación

Realizar pruebas unitarias y de integración, subiendo documentos simulados y verificando que los eventos **se generen** correctamente. Se **probarán** casos como:

- Subir un documento y luego **consultarlo**.
- Intentar subir un hash inválido y **verificar** que el contrato **rechace** la operación.
- Intentar eliminar un documento como usuario no autorizado y **confirmar** que la protección **funcione** correctamente.

Estas pruebas **permitirán** demostrar que el sistema **funcionará** de manera confiable y que los registros en la blockchain **garantizarán** la autenticidad de los documentos.

A continuación, en la tabla [1] se muestra de manera general las actividades que se realizarán.

Tabla 3: Actividades Metodología Scrum

Sprint	Actividades

Análisis de requisitos	**Identificar** problemas y **definir** requisitos funcionales y no funcionales
Diseño del Sistema	Diseño Arquitectura de Contrato Inteligente Definir la Estructura de Base de Datos Prototipado y Desarrollo de Frontend en React
Selección de Tecnologías	Servicios de Solidity, React, Node.js e IPFS simulado
Desarrollo del Sistema	Implementar funciones y manejador de eventos
Pruebas y Validación	**Ejecución de** pruebas unitarias, de integración, validación de eventos y permisos
Desarrollo del Subsistema de Reportes y Visualización	Generación de Reportes Visualización de Datos
Documentación	**Registrar** hallazgos, procedimientos y recomendaciones para futuras implementaciones

1.7. Factibilidad

La viabilidad de este proyecto se sustenta, en gran medida, en una planificación financiera cuidadosa. A continuación, se detallan los costos previstos para su ejecución.

1.7.1. Factibilidad Técnica

Para el desarrollo del proyecto se **requerirán** los siguientes recursos técnicos:

- **Equipos de cómputo:** se **utilizarán** computadoras con capacidad suficiente para ejecutar entornos de desarrollo, simulaciones de blockchain local y pruebas de frontend.
- **Software y entornos de desarrollo:**

- **Visual Studio Code:** se **empleará** para desarrollar el frontend en React y para escribir scripts de interacción con la blockchain.
- **Node.js y npm:** se **utilizarán** para gestionar dependencias y ejecutar el servidor local del frontend.
- **Solidity y Hardhat/Remix:** se **utilizarán** para desarrollar, compilar y probar el contrato inteligente (DocumentStorage) en la blockchain local.
- **IPFS simulado:** se **implementará** para almacenar hashes de documentos y simular la distribución de archivos.

- **Red Blockchain local:** se **configurará** un entorno privado que permita probar la autenticación de documentos sin depender de nodos externos o servicios en la nube.

Este conjunto de recursos **permitirá** crear, registrar y verificar documentos de manera segura, simulando un entorno real, y **asegurará** que todos los procesos puedan probarse antes de una posible implementación institucional.

1.7.2. Factibilidad Operativa

El proyecto **será ejecutado** por la estudiante **Ivan Rodriguez y** , quien cuenta con los conocimientos en desarrollo frontend con React, manejo de Solidity y pruebas de blockchain local. Además, **se contará** con asesoría de un docente experto en tecnologías blockchain para resolver dudas y orientar sobre buenas prácticas en el desarrollo de contratos inteligentes y seguridad de la información.

El proceso operativo **se desarrollará** siguiendo la metodología SCRUM, con iteraciones planificadas para cada sprint, garantizando que cada fase —desde análisis de requisitos hasta pruebas y documentación— **se cumpla** de manera organizada y controlada.

1.7.3. Factibilidad Económica

El costo de la ejecución del proyecto se basa en lo siguiente:

- El costo de los dos equipos de cómputo y hosting requeridos para el desarrollo del sistema planteado
- El costo de la mano de obra de cada uno de los integrantes que desarrollara la propuesta • El costo de las asesorías del tutor

Las siguientes tablas [2], [3] y [4] muestran el total de costos en el siguiente orden: recursos humanos, técnicos y costo total.

Tabla 4: Factibilidad Económica - Mano de Obra

Integrante	Descripción	Valor Hora	Horas	Total
Desarrolladores	Ivan Rodriguez Shanexon Ortiz	$ 60.000	40	$ 6’000.000
Tutor	Asesor en Blockchain	$ 80.000	20	$1’200.000
				Total **$ 7’200.00**

Tabla 5: Factibilidad Económica - Recursos Técnicos

Integrante	Descripción	Cantidad	Valor	Total
Desarrolladores	Computadora personal para desarrollo y pruebas	2	2’500.000	$ 5’000.000
Software y herramientas	VSCode, Node.js, Remix, IPFS simulado	1		$0
	Total			**$ 5’000.00**

Tabla 6: Factibilidad Económica - Costo Total

Concepto	Total
Recursos Humanos	$ 7’200.000
Recursos Técnicos	$ 5’000.000
Subtotal	**$ 12’200.000**
Imprevistos (10%)	$ 300.000
Total	**$ 12’500.000**

1.7.4. Factibilidad Legal

Desde el punto de vista legal, el proyecto **se desarrollará** completamente en un **entorno local**, sin conexión a redes públicas ni intercambio de datos con terceros. Esto **garantiza** que no se infringirán normativas de protección de datos personales, ya que todos los documentos utilizados **serán simulados** y no contendrán información sensible real de estudiantes o profesores.

Se **tomará en cuenta** la legislación colombiana vigente sobre propiedad intelectual y protección de datos, especialmente lo relacionado con el manejo de información académica y la autenticación de documentos. Por ejemplo, la Ley 1581 de 2012 sobre Protección de Datos Personales **marca que cualquier tratamiento de información de personas debe ser autorizado**, y como este proyecto **no manejará información real**, se **cumplirá** de manera indirecta con dichos lineamientos.

Asimismo, el proyecto **respetará** las normas de propiedad intelectual al emplear tecnologías como **Solidity, React y Node.js**, las cuales se encuentran bajo licencias abiertas o gratuitas. Esto **asegura** que no se presenten conflictos legales por el uso del software, y que cualquier código desarrollado **podrá ser reutilizado** dentro del marco académico sin problemas.

Se **considerará** también que, al tratarse de un prototipo académico, **no se hará implementación comercial** ni distribución externa del sistema, lo que **minimiza riesgos legales**

y permite enfocarse en demostrar la factibilidad técnica y operativa del proyecto. En pocas palabras, este proyecto **funcionará como un laboratorio**, un espacio seguro para experimentar con la autenticación de documentos en blockchain, sin comprometer datos reales ni violar leyes existentes.

En resumen, la factibilidad legal **está asegurada**, ya que todas las acciones **se desarrollarán dentro del ámbito académico**, con datos simulados y respetando las licencias de software y la normativa nacional. Esto **permite avanzar** con la investigación y el desarrollo del prototipo sin preocupaciones legales, enfocándose en probar conceptos y demostrar cómo la blockchain **puede aportar valor** en la autenticación de documentos.

1.8. Cronograma

En la ilustración [1] se presenta el cronograma de actividades.

Ilustración 1:Cronograma

Responsable del proyecto

Inicio del proyecto: dom, 2025-06-15

Semana para mostrar: 1

16 de junio de 2025 | 23 de junio de 2025 | 30 de junio de 2025 | 7 de julio de 2025 | 14 de julio de 2025 | 21 de julio de 2025 | 28 de julio de 2025 | 4 de agosto de 2025

TAREA	ASIGNADO A	PROGRESO	INICIO	FIN
Fase 1 – Análisis y Planificación				
Revisión del proceso actual de emisión y verificación de certificados académicos.	Ivan Rodriguez	80%	15-6-25	18-6-25
Identificación de tiempos de respuesta, riesgos de seguridad y puntos críticos.	Shanexon Ortiz	80%	18-6-25	20-6-25
Definición de requerimientos funcionales y técnicos del prototipo.	Shanexon Ortiz	100%	20-6-25	24-6-25
Fase 2 – Investigación y Diseño				
Investigación de tecnologías blockchain y opciones de red privada/local.	Shanexon Ortiz	100%	25-6-25	29-6-25
Evaluación de librerías y herramientas para integración con IPFS.	Ivan Rodriguez	100%	27-6-25	2-7-25
Selección de los componentes técnicos más adecuados.	Shanexon Ortiz	100%	2-7-25	5-7-25
Diseño de la arquitectura del sistema.	Ivan Rodriguez	100%	2-7-25	4-7-25
Diseño del contrato inteligente para registrar hashes de documentos.		100%	2-7-25	5-7-25
Fase 3 – Desarrollo del Prototipo				
Configuración del entorno local de desarrollo.	Ivan Rodriguez	100%	30-6-25	5-7-25
Programación del contrato inteligente en Solidity.	Shanexon Ortiz	100%	6-7-25	10-7-25
Configuración de IPFS en entorno local.	Ivan Rodriguez	100%	11-7-25	16-7-25
Desarrollo de la interfaz web (subida y búsqueda de documentos).	Shanexon Ortiz	100%	17-7-25	21-7-25
Integración entre frontend, backend, blockchain e IPFS.	Ivan Rodriguez	100%	11-7-25	31-7-25
Fase 4 – Pruebas y Presentación				
Pruebas funcionales del prototipo con casos simulados.	Shanexon Ortiz	100%	1-8-25	21-8-25
Pruebas de rendimiento y seguridad en entorno controlado.	Shanexon Ortiz	20%	1-8-25	21-8-25
Documentación técnica y manual de usuario.	Ivan Rodriguez	100%	1-1-00	21-1-00

Fuente: Elaboración propia

Capítulo 2

Análisis

2.1. Análisis de Requerimientos

Para el desarrollo del proyecto de **autenticación de documentos mediante blockchain**, se **identificarán** y **definirán** los requerimientos necesarios para garantizar que el sistema cumpla con su propósito. Este análisis **permitirá** establecer qué funcionalidades serán implementadas y qué características deberán cumplir en cuanto a rendimiento, seguridad y usabilidad.

Se **tomará como referencia** la problemática detectada en la Universidad Distrital Francisco José de Caldas, donde se presentan dificultades para verificar la autenticidad de

documentos académicos y se requiere un sistema confiable que **permita** a los usuarios comprobar de manera inmediata si un documento es válido o no.

El análisis se **dividirá** en dos grandes categorías: **requerimientos funcionales** y **requerimientos no funcionales**. Los primeros describen lo que el sistema **hará**, mientras que los segundos establecen **cómo debe comportarse** y con qué estándares debe operar.

2.1.1. Requerimientos Funcionales

Tabla 7: Registro de Documentos

ID	RF 01
Nombre	Registro de Documentos
Descripción	El sistema **permitirá** que los usuarios suban documentos al contrato inteligente, generando un hash único que será registrado en la blockchain local junto con la fecha y hora de registro.
Actores	Administrador, Estudiante
Observaciones	Cada documento **se asociará** a la dirección del usuario que lo sube, garantizando trazabilidad y autenticidad. El administrador podrá supervisar la correcta subida de los documentos.

Tabla 8: Registro de Eventos

ID	RF 02
Nombre	Registro de Eventos
Descripción	Cada acción de subida o eliminación de documentos **generará** un evento que se almacenará en la blockchain local, permitiendo auditar las acciones de los usuarios.
Actores	Estudiante, Administrador
Observaciones	Los eventos **facilitarán** la verificación del historial de documentos sin necesidad de consultar directamente los datos sensibles de los archivos.

Tabla 9: Consulta de Documentos

ID	RF 02
Nombre	Consulta de Documentos
Descripción	Los usuarios **podrán** consultar los documentos que han sido registrados, verificando su hash y timestamp para asegurar su autenticidad.
Actores	Estudiante, Profesor, Administrador
Observaciones	La consulta **permitirá** que cualquier actor autorizado confirme la existencia y validez de un documento sin necesidad de acceder a la información sensible del contenido del archivo.

2.1.2. Requerimientos No Funcionales

Los requerimientos no funcionales **describirán** cómo se **deberá comportar** el sistema más allá de las funcionalidades básicas. Es decir, no se enfocarán en **qué hará** la aplicación, sino en **cómo lo hará**, asegurando que cumpla con estándares de rendimiento, seguridad, confiabilidad y experiencia de usuario.

En este proyecto, se **considerarán** aspectos como la seguridad de los documentos, la integridad de los datos, la facilidad de uso, la disponibilidad de las funciones y la escalabilidad del sistema para soportar un número creciente de documentos y usuarios. Por ejemplo, aunque todo se **ejecutará** en un entorno local y con datos simulados, se **probará** que las funciones respondan de manera rápida y que los documentos registrados sean inalterables, garantizando la confiabilidad del prototipo.

Además, se **buscará** que la interfaz sea intuitiva, de manera que cualquier estudiante, profesor o administrador pueda interactuar con el sistema sin complicaciones técnicas, y que los procesos críticos, como la subida o verificación de documentos, **mantengan** la integridad y

trazabilidad de la información. En pocas palabras, estos requerimientos no funcionales **aseguraran** que el sistema no solo funcione, sino que lo haga de manera eficiente, segura y confiable.

Tabla 10: Disponibilidad y Rendimiento

ID	RNF 01
Nombre	Disponibilidad y Rendimiento
Descripción	El sistema **deberá** responder de manera rápida ante las consultas y subidas de documentos, simulando un entorno estable y confiable en la blockchain local.
Observaciones	Aunque todo se **ejecutará** en entorno local, se **probará** que las funciones **responden** en tiempos adecuados, asegurando una experiencia de usuario fluida.

Tabla 11: Escalabilidad

ID	RNF 2
Nombre	Escalabilidad
Descripción	El sistema **deberá** permitir la incorporación de nuevos usuarios y documentos sin afectar significativamente el rendimiento de las consultas o registros. Aunque todo se **ejecutará** en entorno local, la arquitectura **será diseñada** pensando en un posible crecimiento futuro.
Observaciones	Se **probará** la respuesta del sistema con diferentes volúmenes de documentos y usuarios simulados, asegurando que la experiencia siga siendo fluida y confiable.

Tabla 12: Integridad de Datos

ID	RNF 3
Nombre	Integridad de los Datos

Descripción	Todos los documentos **deberán** permanecer inalterables una vez registrados en la blockchain local. Esto **asegurará** que los registros no puedan ser modificados de manera fraudulenta y que los hashes de los documentos sean confiables.
Observaciones	Cada subida de documento **registrará** un hash único y timestamp, permitiendo verificar que el contenido no fue alterado desde su registro inicial.

2.1.3. Definición de actores

Según el análisis de requerimientos los actores implicados en este proyecto se presentan en las tablas [11] y [12] de la siguiente manera:

Tabla 13: Actor - Administrador

Nombre	Administrador
Descripción	Es el encargado de supervisar y gestionar todo el sistema de autenticación de documentos. Esto incluye crear y administrar usuarios, asignar permisos de acceso a distintos roles (por ejemplo, estudiantes, docentes o evaluadores), y garantizar que los documentos subidos a la blockchain se registren correctamente. Además, monitorea el rendimiento del sistema y verifica la integridad de los documentos almacenados, asegurando que toda la información sea segura y confiable.
Atributos	Nombres, Apellidos, clave, correo.

Tabla 14:Actor - Estudiante

Nombre	Estudiante

Descripción	Es el usuario que genera y gestiona sus propios documentos dentro del sistema. Su función principal es subir documentos académicos a la blockchain, revisar que se hayan registrado correctamente y verificar la autenticidad de sus propios archivos. También puede solicitar correcciones o actualizaciones de documentos en caso de errores, y consultar el estado de verificación de los documentos en tiempo real. Su interacción asegura que el flujo de autenticación funcione de manera correcta desde la perspectiva del usuario final.
Atributos	Nombres, Apellidos, clave, correo, proyecto curricular.

Capítulo 3

Diseño

3.1. Solución Tecnológica

La propuesta tecnológica de este proyecto gira en torno a un sistema diseñado para **registrar, almacenar y autenticar documentos universitarios**, como diplomas, certificados y demás documentos académicos. La idea principal es garantizar que cada documento sea **inmutable, verificable y accesible de manera segura**, evitando manipulaciones o falsificaciones.

A diferencia de los sistemas tradicionales, donde toda la información depende de un servidor central —y, seamos sinceros, cualquier falla o ataque puede comprometer todo—, aquí se emplea **blockchain** junto con **IPFS**. Esto significa que cada documento obtiene un **identificador único llamado CID**, que se almacena en la blockchain local. Así, cualquier consulta sobre la autenticidad del documento puede realizarse de manera confiable, rápida y sin intermediarios.

Todo el proyecto se ejecuta **en un entorno local**, lo que ofrece varias ventajas: control total sobre los datos de prueba, facilidad para depurar errores y, además, permite experimentar libremente sin depender de servicios externos. Es como tener un pequeño laboratorio propio, donde puedes probar ideas y comprobar resultados al instante.

3.1.1 Componentes del sistema

El proyecto funciona sobre un entorno controlado que integra:

- **Blockchain local** (Ganache o Hardhat), que permite desplegar y probar los smart contracts sin riesgos externos.
- **Truffle**, para compilar, migrar y testear los contratos inteligentes.
- **IPFS local o Pinata**, encargado de almacenar los archivos de manera descentralizada y generar los CIDs únicos.

Imagínalo como un taller: tienes todas las herramientas a la mano, puedes probar cada pieza y asegurarte de que encaje perfectamente antes de abrir la tienda al público.

3.1.1.1 Smart Contracts

El contrato inteligente es la columna vertebral del sistema:

- **Registrar documentos**: función storeDocument que guarda el CID en la blockchain.
- **Verificar autenticidad**: función verifyDocument que permite consultar si un documento ha sido registrado correctamente.

Cada línea de código está pensada para garantizar seguridad e inmutabilidad. No hay espacio para improvisaciones; la blockchain se encarga de validar todo.

3.1.1.2 Interfaz de usuario

El sistema cuenta con un frontend diseñado para ser intuitivo y accesible, de manera que cualquier usuario pueda interactuar con la aplicación sin necesidad de conocimientos técnicos avanzados en blockchain. La interfaz permite, en primer lugar, la **subida de documentos académicos**, donde cada archivo cargado genera automáticamente un identificador único (CID) mediante IPFS. Este proceso se realiza de forma transparente para el usuario, lo que asegura simplicidad en el uso y, al mismo tiempo, solidez en la gestión de datos.

Otra funcionalidad central es la **verificación de documentos**. El usuario tiene la posibilidad de comprobar la validez de un archivo académico ingresando directamente el documento o utilizando el CID correspondiente. De esta manera, se garantiza que la autenticidad del registro pueda confirmarse de forma rápida y confiable, reduciendo los riesgos de manipulación o fraude.

Finalmente, la interfaz ofrece un **módulo de consulta de historial**, donde se muestran de manera organizada todos los documentos previamente registrados. Cada entrada incluye información relevante como la fecha de carga, el CID generado y el estado de verificación del archivo. Este componente no solo aporta transparencia en el manejo de la información, sino que también facilita la trazabilidad de los documentos, permitiendo a los usuarios mantener un control claro de sus registros académicos.

.

3.1.2 Características del sistema

El sistema desarrollado presenta un conjunto de características que refuerzan su valor como propuesta tecnológica para la autenticación de documentos académicos. En primer lugar, se destaca su **naturaleza descentralizada**, ya que los archivos no dependen de un único servidor centralizado, sino que se distribuyen en una red de nodos, lo cual reduce riesgos asociados a fallos técnicos o intentos de manipulación.

Otra propiedad fundamental es la **inmutabilidad**. Una vez que un documento ha sido registrado en la blockchain, su información no puede ser alterada sin dejar rastro en el historial de transacciones. Esto garantiza que los registros académicos conserven su validez en el tiempo y refuerza la confianza tanto para estudiantes como para terceros que requieran verificarlos.

De igual manera, el sistema ofrece **seguridad, trazabilidad y transparencia**. La integración de IPFS con blockchain permite que cada documento posea un identificador único verificable en cualquier momento, lo cual asegura su resistencia a fraudes. Además, todas las operaciones quedan registradas en la cadena de bloques, lo que facilita procesos de auditoría y aumenta la credibilidad institucional al permitir que cualquier interacción pueda ser consultada de manera abierta y verificable.

3.1.3. Herramientas de desarrollo utilizadas

El desarrollo del sistema requirió integrar diversas herramientas que, en conjunto, permiten construir una solución robusta, escalable y fácil de usar. La elección de cada una no fue arbitraria, sino que respondió a criterios de compatibilidad, soporte técnico y pertinencia para los objetivos del proyecto.

En primer lugar, se empleó **Visual Studio Code (VS Code)** como entorno de desarrollo. Su flexibilidad, sumada a la gran cantidad de extensiones para **Solidity y JavaScript,** facilitó el trabajo con contratos inteligentes, scripts de automatización y el diseño del frontend. Esta elección se justifica porque ofrece en un mismo espacio todas las herramientas necesarias para el desarrollo full stack, reduciendo la curva de aprendizaje y el tiempo de depuración**.**

Para simular la red blockchain se utilizaron Ganache y Hardhat, ambos ampliamente adoptados en el ecosistema Ethereum. Estas plataformas permiten desplegar nodos locales, generar cuentas de prueba y observar en detalle cada transacción. De esta manera, se pudo garantizar que el sistema fuera validado en un entorno seguro antes de su implementación en una red real, lo que disminuye riesgos y asegura un desarrollo más controlado**.**

El almacenamiento de los documentos se resolvió con **IPFS (InterPlanetary File System),** dado que la blockchain por sí sola no resulta adecuada para guardar archivos completos. IPFS permite generar identificadores únicos para cada documento, asegurando que cualquier modificación sea detectable de inmediato. Para una gestión más sencilla, se contempló también el uso de **Pinata,** que ofrece una interfaz más amigable para interactuar con IPFS sin comprometer su carácter descentralizado. La combinación de ambas herramientas asegura que los certificados no dependan de un servidor central y permanezcan disponibles de forma permanente.

Finalmente, el frontend se desarrolló en **React,** por su arquitectura basada en componentes y su facilidad para crear interfaces dinámicas. Esto permitió diseñar módulos independientes —como formularios de carga de certificados o paneles de verificación— que luego se integraron de manera coherente en la aplicación. React también ofrece gran compatibilidad con bibliotecas externas, lo que facilitó la comunicación fluida con la API conectada a blockchain e IPFS**.**

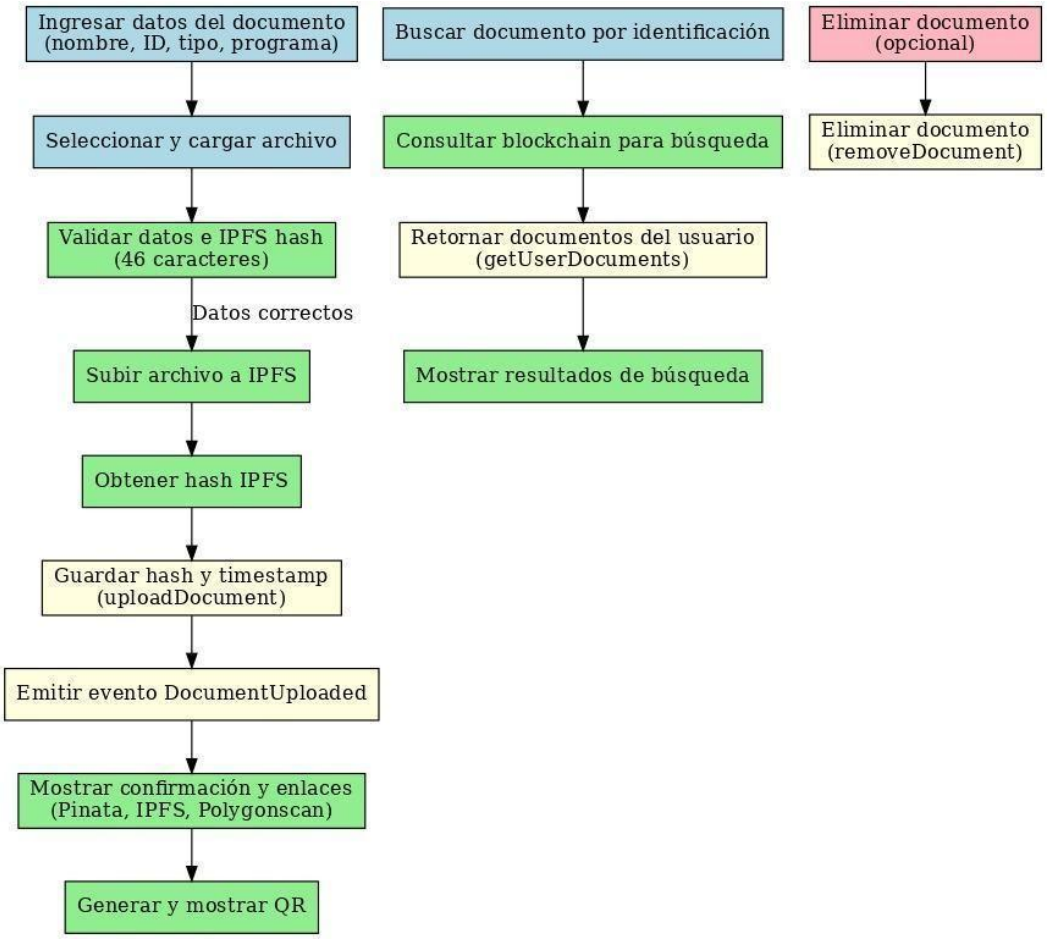
En conjunto, estas herramientas garantizan que el sistema sea consistente, seguro y usable, cumpliendo con la meta de ofrecer a los estudiantes y empleadores de la Universidad Distrital un mecanismo de validación confiable y moderno.

3.2. Diagrama de Procesos

Representación Gráfica Flujo Desarrollo

En la ilustración [2] la interacción entre el usuario, la aplicación y la cadena de bloques. El diseño se estructura en tres procesos principales: la **carga de documentos**, la **búsqueda de documentos** y la **eliminación opcional de documentos**.

Ilustración 2: Representación Flujo - Grafico



Fuente: Elaboración propia

Diagrama de Flujo – Sistema de Gestión de Documentos Blockchain

En la ilustración [3] El diagrama ilustra el flujo completo del sistema propuesto para la gestión y validación de documentos mediante tecnología blockchain, representado en formato swimlanes para diferenciar claramente las responsabilidades de cada actor. Se identifican cuatro participantes principales:

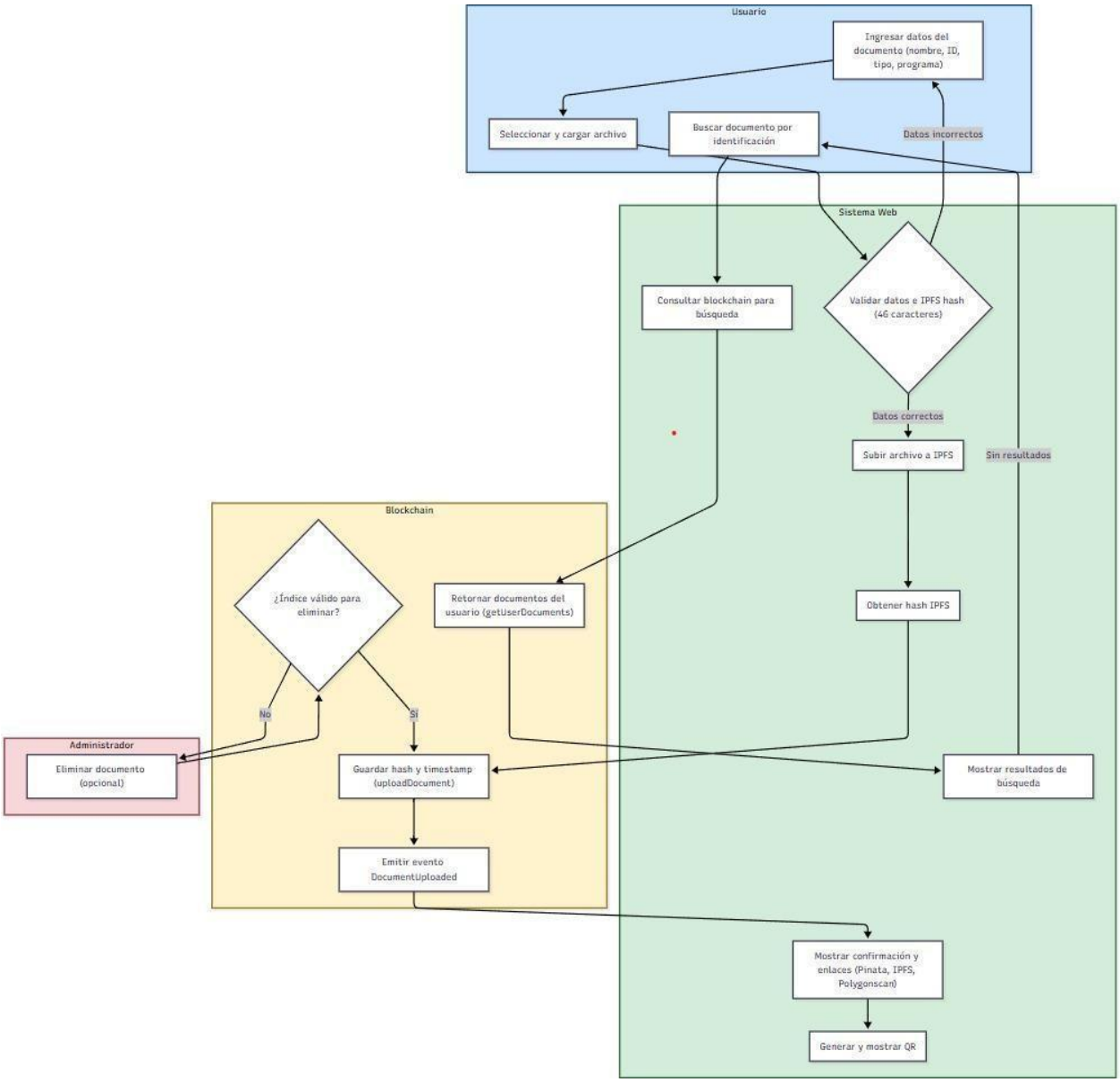
- **Usuario**: encargado de ingresar los datos del documento, seleccionar y cargar el archivo, así como realizar consultas por número de identificación.

- **Sistema Web**: encargado de validar los datos ingresados, interactuar con la red IPFS para almacenar el archivo, obtener su hash y comunicarse con la blockchain para registrar la información. También genera enlaces de consulta y códigos QR para facilitar el acceso a los documentos.
- **Blockchain**: mediante un contrato inteligente desarrollado en Solidity, almacena de forma inmutable el hash y la fecha de registro del documento, emite eventos para notificar acciones y responde a solicitudes de consulta o eliminación de documentos.
- **Administrador**: rol opcional con privilegios para eliminar documentos en casos específicos.

El flujo incluye condicionales y ciclos para manejar casos de error o validación fallida, como cuando los datos no cumplen con el formato requerido (por ejemplo, un hash IPFS de longitud incorrecta) o cuando no se encuentran resultados en una consulta. Estos ciclos permiten que el proceso regrese a pasos anteriores, garantizando que solo se almacene información válida y que las búsquedas sean efectivas.

Este diagrama refleja la interacción entre las capas del sistema, la lógica de negocio implementada en el contrato inteligente y la integración con IPFS, asegurando trazabilidad, integridad y disponibilidad de los documentos.

Ilustración 3: Diagrama de Flujo Sistema de Gestión de Documentos Blockchain

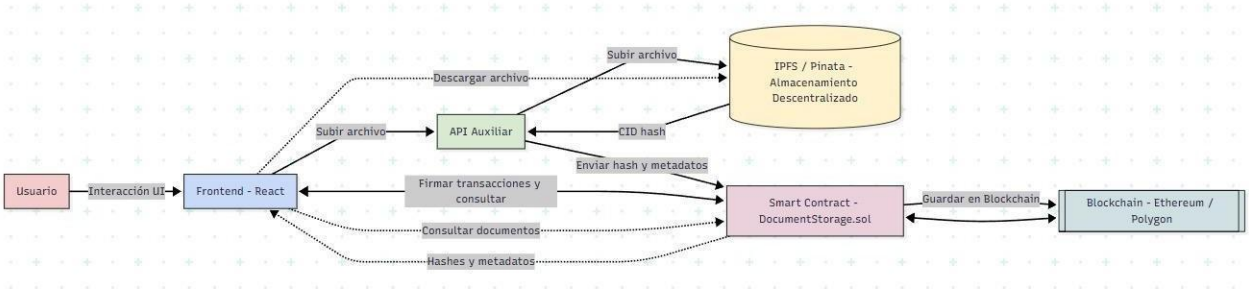


Fuente: Elaboración propia

3.3. Diagrama de Arquitectura

A continuación, se presenta el diagrama de arquitectura del sistema que se basa en un modelo híbrido que combina componentes centralizados auxiliares con una infraestructura descentralizada para garantizar integridad, transparencia y resistencia a la manipulación de datos.

Ilustración 4: Diagrama de Arquitectura



Fuente: Elaboración propia

Este diseño elimina la dependencia de servidores centralizados para el almacenamiento de datos críticos, ya que la información principal (hash del documento y metadatos) reside en la blockchain y el archivo en IPFS, garantizando así la descentralización y la integridad de la información.

3.3.1. Capa de Usuario (Front-end / Interfaz de usuario)

En el presente proyecto, la capa de usuario se ejecuta principalmente en un entorno local y de pruebas, con el fin de facilitar el desarrollo, la validación y el análisis del funcionamiento del sistema sin depender de infraestructuras externas. La aplicación frontend se conecta a una red blockchain local o a redes de prueba (testnet), lo que permite simular escenarios reales de uso sin incurrir en costos ni riesgos asociados a entornos de producción.

Durante esta fase experimental, los documentos y registros generados son almacenados de manera controlada mediante IPFS y gestionados a través del contrato inteligente desplegado en la red de pruebas, garantizando así la integridad y disponibilidad de la información en un contexto académico. Este enfoque permite evaluar el desempeño del sistema, identificar fallos y realizar ajustes antes de una posible implementación institucional.

Adicionalmente, la arquitectura propuesta contempla la posibilidad de una futura migración a infraestructuras en la nube, como Azure o AWS, en caso de que el sistema sea adoptado de manera oficial. En dicho escenario, podrían implementarse mecanismos de almacenamiento redundante y alta disponibilidad para asegurar la continuidad del servicio. No obstante, en el alcance actual del proyecto, el énfasis se centra

en la validación técnica mediante entornos locales y redes de prueba, priorizando el aprendizaje, la experimentación y la demostración de la viabilidad del sistema.

3.3.2. Capa de Lógica / Aplicación (Back-end / Smart Contracts)

En esta capa se concentra el procesamiento de las solicitudes de los usuarios y la aplicación de las reglas de negocio que estructuran el sistema. Aquí se encuentran los *smart contracts*, que funcionan como programas autónomos y confiables encargados de gestionar la

autenticación y el registro de documentos académicos. Cuando un administrador carga un certificado previamente emitido por la universidad, el contrato inteligente genera un hash único del archivo y lo guarda en la blockchain. Más adelante, cuando alguien necesita verificar ese documento, el sistema compara el hash calculado con el que está registrado en la red; si no coinciden, la validación se rechaza de inmediato. Esta capa también administra los permisos de acceso, estableciendo de manera clara quién puede registrar información en la cadena y quién solo puede consultarla, lo que refuerza la seguridad y previene manipulaciones indebidas. Para su implementación se propone el uso de **Node.js** y **JavaScript** en el desarrollo del **back-end**, mientras que los contratos inteligentes se desarrollan en **Solidity** y se despliegan en una red de pruebas local como **Ganache**.

3.3.3. Capa de Blockchain / Registro Distribuido

Esta capa tiene como finalidad almacenar de manera inmutable la información crítica del sistema, en particular los hashes de los documentos, los cuales funcionan como identificadores únicos que garantizan la integridad de los certificados. Sin embargo, no toda la información requiere almacenarse en blockchain, pues esto resultaría poco eficiente. Por esa razón, los metadatos adicionales —como el nombre del estudiante, el tipo de documento o la fecha de emisión— pueden resguardarse en una base de datos complementaria, lo que permite realizar búsquedas rápidas y consultas internas sin comprometer la seguridad. De esta forma se consigue un equilibrio entre la **inmutabilidad** que ofrece blockchain y la **agilidad** de un sistema de gestión de datos tradicional. Para estas funciones, se consideran tecnologías como SQLite, PostgreSQL o MongoDB, que brindan flexibilidad en pruebas y escalabilidad para escenarios más amplios..

3.3.4. Integración / API

La capa de integración funciona como un puente entre la interfaz de usuario y la lógica del sistema basada en contratos inteligentes. Su papel es esencial, ya que recibe las solicitudes de **registro o verificación** de documentos, las traduce en llamadas hacia los *smart contracts* y devuelve una respuesta clara y comprensible al usuario final. Por ejemplo, cuando un empleador consulta un certificado, la API procesa la petición, se comunica con la blockchain y responde con un mensaje como “Documento autenticado” o “Documento no válido”. De esta manera, el

usuario no necesita enfrentarse a la complejidad técnica de la blockchain, sino que obtiene una experiencia sencilla, confiable y eficiente. Para la construcción de esta capa se recomiendan herramientas como Node.js con Express, que facilitan la creación de servicios web, y librerías como Web3.js o Ethers.js, diseñadas específicamente para la interacción con la blockchain.

Capítulo 4

Implementación

4.1. Infraestructura local / Entorno de desarrollo

Para la implementación del sistema de autenticación de documentos universitarios mediante blockchain e IPFS, se utilizó un **entorno de desarrollo completamente local**, lo que permitió un control total sobre todos los componentes del proyecto y la posibilidad de

experimentar sin depender de servicios externos. Esto fue fundamental para garantizar la **confidencialidad de los datos de prueba** y para poder depurar errores de manera inmediata.

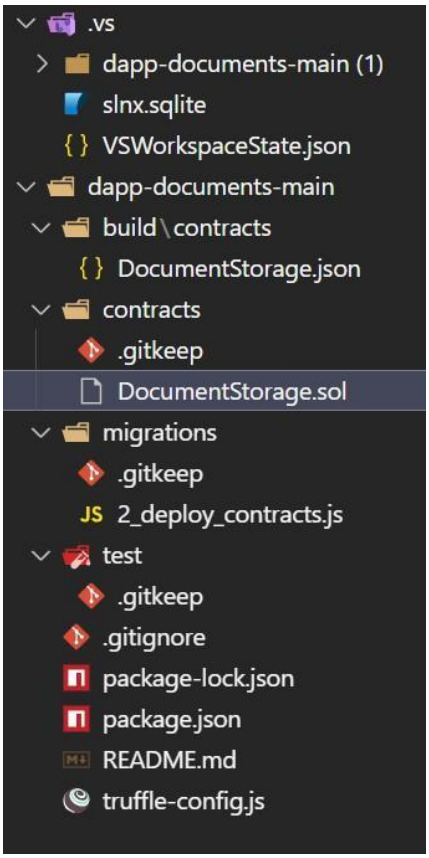
4.1.1. Estructura de carpetas

La organización del proyecto se llevó a cabo siguiendo buenas prácticas de desarrollo en aplicaciones blockchain, con el propósito de mantener una estructura clara y modular. En el directorio **contracts** se ubican los *smart contracts* del sistema, entre ellos *DocumentStorage.sol*, encargado de gestionar el registro y la verificación de documentos dentro de la red. La carpeta **migrations** contiene los scripts responsables de desplegar estos contratos en la blockchain local, mientras que en **build/contracts** se almacenan los artefactos generados por Truffle tras el proceso de compilación. Finalmente, el directorio **test** reúne las pruebas unitarias que permiten validar el correcto funcionamiento de los contratos y de sus interacciones con la red.

Este tipo de organización no solo facilita la comprensión del proyecto por parte de otros desarrolladores, sino que también contribuye al mantenimiento y a la escalabilidad futura, al mantener cada componente claramente separado según su función.

.

Ilustración 5: Estructura Carpetas



Fuente: Elaboración propia

4.1.2. Blockchain local

Para llevar a cabo las pruebas del sistema se configuró una **blockchain local** utilizando herramientas como **Ganache** y, en algunos casos, **Hardhat**, que permiten simular de manera sencilla el comportamiento de una red real en un entorno controlado. Con esta configuración es posible levantar nodos de prueba, generar cuentas ficticias y ejecutar transacciones sin necesidad de utilizar criptomonedas reales ni exponer el sistema a riesgos externos.

El uso de una red local resulta especialmente útil en fases de desarrollo, ya que permite verificar el funcionamiento de los contratos inteligentes y del proceso de registro de documentos antes de migrar a un entorno de producción. De esta manera, cada transacción realizada —como el almacenamiento del hash de un certificado académico— puede revisarse y validarse en un entorno seguro, asegurando la integridad y la inmutabilidad de los datos sin incurrir en costos ni depender de una red pública.

4.1.3. IPFS local o en Pinata

El sistema no almacena directamente los documentos en la blockchain, ya que esto sería poco eficiente en términos de costos y capacidad. En su lugar, se utiliza el **Sistema de Archivos Interplanetario (IPFS)**, que permite guardar los archivos de manera descentralizada y generar para cada uno un identificador único denominado **CID** (*Content Identifier*). Este código funciona como una huella digital que garantiza que el archivo no ha sido modificado, puesto que cualquier alteración cambiaría automáticamente su identificador.

Una vez generado el CID, este se registra en el contrato inteligente desplegado en la blockchain local, estableciendo así un vínculo permanente entre el documento y su registro inmutable en la red. Con este mecanismo se logra combinar la **descentralización del almacenamiento en IPFS** con la **seguridad criptográfica de blockchain**, lo que permite validar la integridad de los certificados académicos en todo momento, incluso cuando se almacenan fuera de la propia cadena de bloques

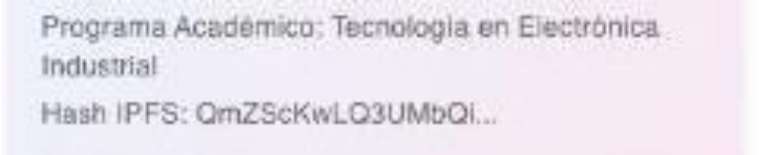
4.2. Almacenamiento de documentos (IPFS)

El almacenamiento de documentos dentro del sistema se implementa a través de **IPFS (InterPlanetary File System)**, una red distribuida que permite guardar archivos de manera descentralizada. Cada documento cargado en la red genera un identificador único denominado **CID (Content Identifier)**, el cual funciona como una referencia inmutable al contenido. De esta forma, los certificados académicos no dependen de un servidor central, sino que pueden consultarse desde múltiples nodos de manera segura y verificable. Este mecanismo resulta esencial para garantizar que los documentos no sean modificados sin que el sistema lo detecte, ya que cualquier alteración en el archivo generaría automáticamente un CID diferente.

4.2.1. Ejemplo práctico de CID

Para validar el funcionamiento, se realizó una prueba con un documento en formato PDF que simulaba un certificado académico. Al subir el archivo a IPFS se generó un CID único, el cual se registró posteriormente en un contrato inteligente desplegado en la blockchain local. Esto permite que, en futuras verificaciones, la autenticidad del documento se compruebe de manera sencilla mediante la comparación entre el **CID** almacenado en la blockchain y el del archivo consultado por el usuario:

Ilustración 6: Generar IPFS



Fuente: Elaboración propia

4.2.2. Consideraciones Finales

El uso de IPFS como sistema de almacenamiento ofrece varias ventajas relevantes para este proyecto. En primer lugar, asegura la **descentralización**, al evitar la dependencia de un servidor único. En segundo lugar, garantiza la **inmutabilidad**, puesto que cada archivo cuenta con un CID irrepetible que se mantiene estable, aunque el documento sea replicado en distintos nodos. Finalmente, proporciona **verificabilidad**, ya que cualquier persona puede comprobar la autenticidad de un documento contrastando su identificador con el registrado en la blockchain. En términos simples, puede decirse que cada archivo posee una “huella digital” propia, que permite reconocerlo de manera inequívoca en cualquier contexto.

4.3. Aplicación / Lógica del sistema

La aplicación desarrollada tiene como propósito principal ofrecer a los usuarios la posibilidad de almacenar y consultar documentos académicos de manera segura, aprovechando la tecnología blockchain y el almacenamiento distribuido. Todo el sistema se ejecuta en un entorno local; no se realizaron integraciones externas más allá de la creación del proyecto. La

interfaz fue construida utilizando **React**, lo que permite una experiencia fluida, dinámica y reactiva para el usuario, donde cada acción genera una respuesta inmediata en la interfaz sin necesidad de recargar la página. A continuación, se desglosa en detalle cómo funciona cada parte de la aplicación, acompañando la descripción con ejemplos del flujo de datos y la interacción entre los componentes.

4.3.1. Interfaz de Carga de Documentos

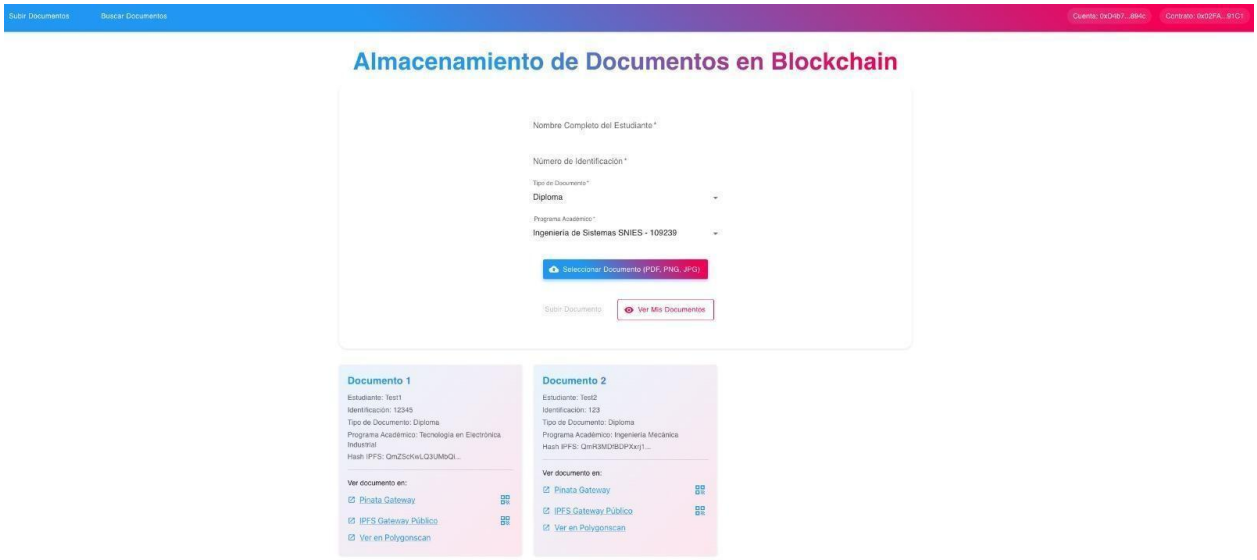
En la sección de **Subir Documentos**, ilustrada en la figura [7], el usuario cuenta con un formulario diseñado para ingresar información personal, seleccionar el tipo de documento —como certificado de notas, diploma o carta de recomendación— y especificar el programa académico correspondiente. Aunque la interfaz resulta sencilla, la lógica implementada en el sistema garantiza la correcta validación y registro de los datos.

Antes de permitir la carga, la aplicación valida que los campos obligatorios, tales como el nombre completo, número de identificación y tipo de documento, estén debidamente diligenciados. En caso contrario, se generan alertas inmediatas que evitan la inserción de información incompleta o inconsistente. Una vez superada esta validación inicial, el sistema habilita la selección de archivos en formatos permitidos (PDF, PNG o JPG) y verifica tanto la compatibilidad como el tamaño, con el fin de asegurar que la subida se realice sin errores.

El archivo validado se envía posteriormente a **IPFS**, donde se genera un identificador único (**CID**) que representa de forma inmutable su contenido. Dicho identificador es registrado en la blockchain local a través de un contrato inteligente, de manera que el documento queda vinculado a un registro seguro y permanente. Este mecanismo garantiza que cualquier modificación posterior pueda ser detectada, ya que alteraría el CID asociado.

Finalmente, la interfaz ofrece al usuario una visualización de los documentos cargados, mostrando información resumida y enlaces para acceder a ellos mediante pasarelas como Pinata Gateway o IPFS Gateway, así como la posibilidad de verificar la transacción en el explorador de la blockchain local. De este modo, el sistema no solo asegura la autenticidad de los archivos, sino que también ofrece transparencia en el proceso y confianza en la gestión de los documentos académicos.

Ilustración 7: Interfaz Carga de Documentos



Fuente: Elaboración propia

4.3.2. Búsqueda de documentos

La sección de **Buscar Documentos**, representada en la ilustración [8], constituye una de las funcionalidades centrales del sistema, ya que permite a los usuarios recuperar de manera rápida y confiable los archivos previamente registrados. Para realizar la consulta, basta con ingresar el número de identificación del estudiante o del titular del documento. Sin embargo, detrás de esta interacción aparentemente sencilla se ejecutan diversos procesos que aseguran la integridad y la trazabilidad de la información.

En primer lugar, la aplicación consulta la blockchain local con el fin de obtener todos los identificadores únicos (**CIDs**) asociados al usuario. Estos CIDs, generados previamente por el sistema de almacenamiento distribuido IPFS, actúan como punteros que enlazan directamente cada documento con su registro en la red. De este modo, el sistema se comporta como un registro oficial digital en el que cada huella corresponde a un documento concreto, lo cual elimina ambigüedades y facilita la localización precisa de la información.

Una vez recuperados los CIDs, la aplicación establece comunicación con la red **IPFS** para obtener los archivos originales. Este paso garantiza que el usuario reciba exactamente la misma

versión del documento que fue cargada en el sistema, sin alteraciones ni modificaciones. La fortaleza de este proceso radica en que, aun si el archivo se replica en múltiples nodos de la red, el identificador único siempre apunta al contenido original, protegiendo así la autenticidad del registro.

El sistema no solo devuelve los archivos, sino que también organiza la información en una interfaz clara y funcional. Cada documento aparece en un listado acompañado de datos complementarios como el tipo de archivo, la fecha de subida y enlaces directos que permiten su verificación en la blockchain o su consulta en diferentes *gateways* de IPFS. Esto amplía las posibilidades de acceso, pues tanto estudiantes como empleadores o instituciones externas pueden corroborar la validez de un certificado en cuestión de segundos.

Finalmente, para hacer aún más práctico el proceso de consulta, cada documento incluye un **código QR** generado automáticamente. Al escanearlo, se redirige al *gateway* correspondiente sin necesidad de copiar cadenas alfanuméricas largas ni tener conocimientos técnicos sobre blockchain o almacenamiento descentralizado. Esta funcionalidad resulta especialmente valiosa en un contexto académico, donde la rapidez y la confiabilidad de la verificación marcan la diferencia entre un trámite exitoso y una oportunidad perdida.

En conjunto, esta sección garantiza que la búsqueda y recuperación de documentos no solo sea posible, sino también transparente, accesible y confiable. La integración de blockchain e IPFS permite que cualquier certificado registrado pueda ser validado con precisión y sin intermediarios, ofreciendo una solución robusta frente a los problemas de manipulación y falsificación de información que afectan a los procesos académicos tradicionales.

Ilustración 8: Interfaz Búsqueda de Documentos



Fuente: Elaboración propia

4.3.3. Visualización y verificación de documentos

En la ilustración [9], se observa cómo la aplicación combina las funciones de subida y consulta, presentando un listado completo de documentos con sus respectivos **hashes de IPFS** y enlaces de verificación. Esta sección demuestra la integración completa de la aplicación:

- **Verificación rápida:** Los usuarios pueden validar la autenticidad de los documentos sin necesidad de tener acceso directo a la blockchain ni conocimientos técnicos avanzados. Solo con escanear el código QR, se obtiene la confirmación de que el archivo no ha sido alterado.
- **Interacción sencilla:** Los documentos se presentan de forma amigable, con botones claros y enlaces funcionales. Esto permite que incluso usuarios menos experimentados puedan utilizar el sistema sin frustraciones.
- **Seguridad y confianza:** La combinación de React para la interfaz, IPFS para el almacenamiento distribuido y blockchain para el registro inmutable genera un entorno robusto y confiable. Cada elemento del sistema trabaja en armonía, asegurando que la información del estudiante esté protegida y que la verificación sea rápida y confiable.

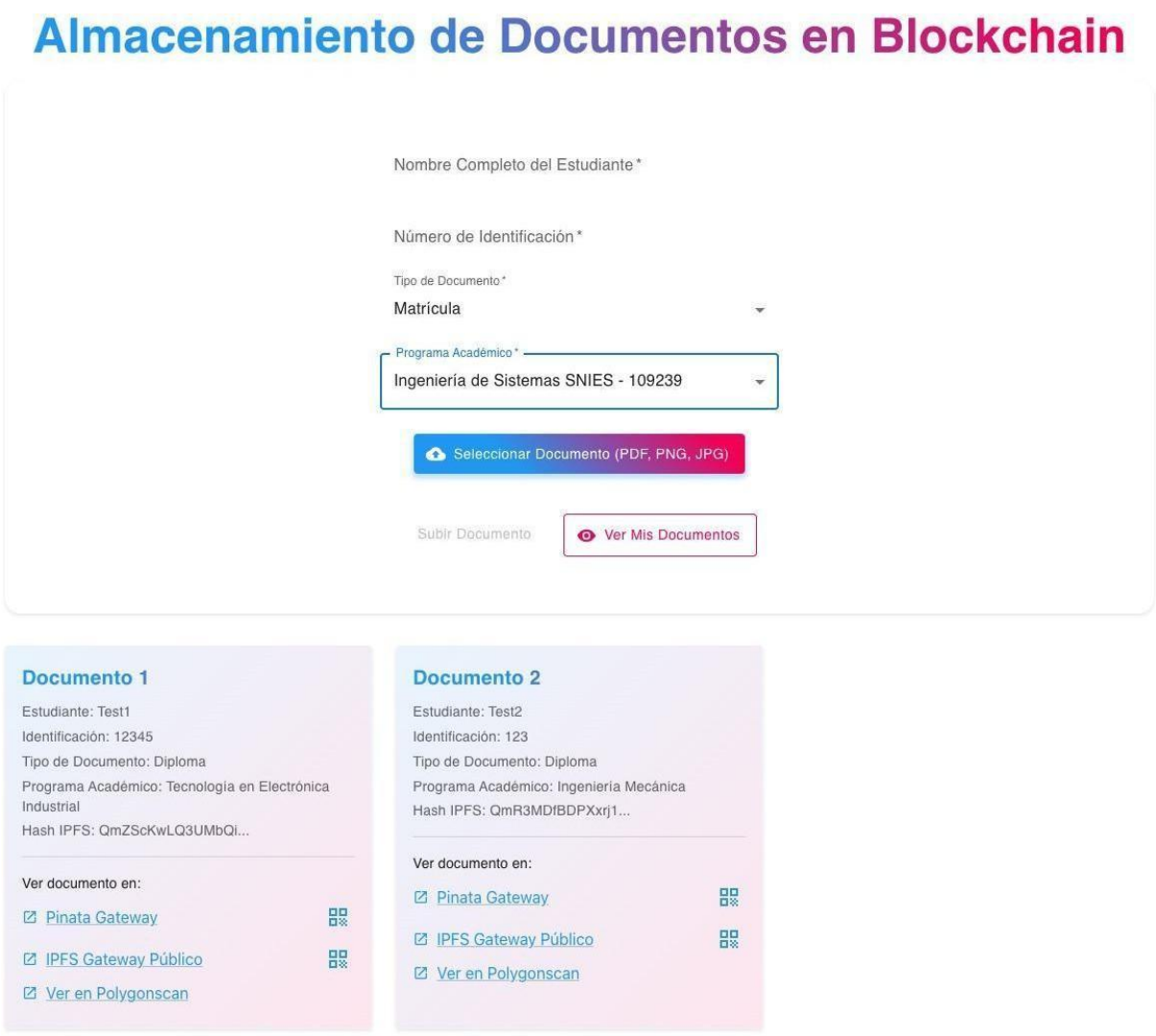
Ilustración 9: Visual Verificación de Documentos



Fuente: Elaboración propia

4.3.4. Flujo de datos y ejemplos prácticos

Para ilustrar un flujo típico: un estudiante sube su diploma en PDF. La aplicación valida su información, sube el archivo a IPFS generando un CID único, y registra este CID en la blockchain local. Cuando un profesor o autoridad académica quiere verificar el diploma, ingresa el número de identificación del estudiante, obtiene el CID, accede al archivo en IPFS y confirma que el hash coincide con el registrado en la blockchain. Todo esto ocurre sin exponer información sensible ni depender de servicios externos, manteniendo la seguridad dentro del entorno local.



Fuente: Elaboración propia

4.4. Smart Contracts / Blockchain

Los **smart contracts** constituyen el corazón del proyecto, ya que son los encargados de registrar y autenticar los documentos universitarios en la blockchain local. En este caso, se desarrolló el contrato DocumentStorage.sol utilizando **Solidity**, permitiendo que cada

documento tenga un **identificador único e inmutable** (CID) y que su autenticidad pueda ser verificada en cualquier momento.

4.4.1. Código del contrato DocumentStorage.sol

El **contrato inteligente DocumentStorage.sol** constituye el núcleo de la lógica de autenticación y registro dentro del sistema propuesto. Su implementación se encuentra en la carpeta *contracts* del proyecto y puede ser inspeccionada a través de un entorno de desarrollo integrado como Visual Studio Code, lo que facilita tanto la revisión del código como su depuración en fases de prueba.

Este contrato incluye una serie de funciones esenciales diseñadas para gestionar de manera segura la relación entre los documentos almacenados en IPFS y los registros inmutables en la blockchain. Una de las funciones principales es **storeDocument**, encargada de recibir el identificador único (CID) generado por IPFS y registrarlo en la cadena de bloques. De esta manera, se establece un vínculo permanente entre el documento original y su referencia en la red, garantizando que no pueda ser modificado sin alterar dicho identificador.

Otra función relevante es **verifyDocument**, la cual permite consultar un CID previamente almacenado y confirmar si el documento correspondiente ha sido registrado de forma correcta. Esta operación resulta fundamental para el proceso de verificación, ya que habilita tanto a usuarios como a entidades externas a corroborar la autenticidad de un archivo sin necesidad de acceder directamente al documento completo.

El contrato también incorpora mecanismos de almacenamiento interno, implementados mediante estructuras de datos como *mappings* y *arrays*, que facilitan la asociación entre usuarios y sus documentos. Con esta organización, el sistema puede manejar múltiples registros por cada usuario, manteniendo un acceso eficiente y seguro a la información.

En conjunto, la lógica contenida en **DocumentStorage.sol** materializa la propuesta de integración entre IPFS y blockchain, ofreciendo una solución práctica y robusta para la gestión de certificados académicos en entornos digitales.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract DocumentStorage {
    // Estructura para almacenar documentos
    struct Document {
        string hash;
        uint256 timestamp;
    }
    // Mapeo para almacenar documentos por usuario
    mapping(address => Document[]) private userDocuments;
    // Eventos para rastrear acciones
    event DocumentUploaded(address indexed user, string hash, uint256 timestamp);
    event DocumentRemoved(address indexed user, uint256 index);
    // Modificador para restringir funciones al propietario del contrato
    modifier onlyOwner() {
        require(msg.sender == owner, "Only the owner can call this function");
        _;
    }
    // Dirección del propietario del contrato
    address public owner;
    constructor() {
        owner = msg.sender; // El creador del contrato es el propietario
    }
```

```
    // Función para subir un documento
    function uploadDocument(string memory _hash) public {
            require(bytes(_hash).length == 46, "Invalid IPFS hash length"); // IPFS hash tiene 46 caracteres
        userDocuments[msg.sender].push(Document({
            hash: _hash,
            timestamp: block.timestamp
        }));
        emit DocumentUploaded(msg.sender, _hash, block.timestamp);
    }
    // Función para obtener documentos de un usuario
    function getUserDocuments(address _user) public view returns (Document[] memory) {
        return userDocuments[_user];
    }
    // Función para eliminar un documento (solo el propietario puede hacerlo)
    function removeDocument(address _user, uint256 _index) public onlyOwner {
        require(_index < userDocuments[_user].length, "Index out of bounds");
        emit DocumentRemoved(_user, _index);
        delete userDocuments[_user][_index];
    }
}
```

4.4.2. Archivo de configuración truffle-config.js

Dentro de cualquier proyecto desarrollado con Truffle, el archivo truffle-config.js cumple un rol fundamental. Este archivo **define cómo y dónde se despliegan los smart contracts**, configurando tanto las redes locales como posibles redes públicas de prueba o mainnets.

```
const HDWalletProvider = require('@truffle/hdwallet-provider');
// Replace or add these lines at the top of the file
const fs = require('fs');
const mnemonic = fs.existsSync(".secret")
  ? fs.readFileSync(".secret").toString().trim()
  : "";
module.exports = {
  networks: {
  development: {
     host: "127.0.0.1",
     port: 8545,
     network_id: "*",
   },
   polygon: {
     provider: () => new HDWalletProvider(
       mnemonic,
       `https://polygon-mainnet.g.alchemy.com/v2/V_kKg5ailXd8p26UTnGzyg78drMHVmSr`
```

```
    ),
    network_id: 137,       // Polygon Mainnet's network id
    confirmations: 2,
    timeoutBlocks: 200,
    skipDryRun: true,
    networkCheckTimeout: 10000,
    maxPriorityFeePerGas: "30000000000", // 30 Gwei
    maxFeePerGas: "100000000000",         // 100 Gwei
    gasLimit: 8000000
   },
  },
 compilers: {
  solc: {
    version: "0.8.0",
    settings: {
    optimizer: {
       enabled: true,
       runs: 200,
      },
    },
   },
  },
};
```

En el desarrollo del proyecto se trabajó principalmente con una **red local de pruebas**, configurada mediante **Ganache**, lo que permitió mantener un control total sobre el proceso de despliegue y depuración de los contratos inteligentes. Esta decisión respondió a la necesidad de contar con un entorno cerrado y seguro, en el que fuera posible ejecutar transacciones ficticias, simular diferentes escenarios de interacción y analizar los resultados sin comprometer recursos económicos reales ni depender de la estabilidad de una red pública. De esta manera, cada fase de prueba pudo ser reproducida de forma confiable, asegurando la correcta validación de la lógica implementada en los contratos.

La configuración de la **red de desarrollo local** fue realizada a través de Truffle, de modo que todos los contratos fueran desplegados en la blockchain simulada que proporciona Ganache. Esto facilitó no solo la gestión de cuentas y direcciones para las pruebas, sino también la verificación del comportamiento de las funciones críticas, como el almacenamiento y consulta de identificadores únicos de documentos (CIDs). Al tratarse de un entorno aislado, cualquier error de programación o de lógica podía ser detectado y corregido sin consecuencias externas, garantizando así un proceso de desarrollo iterativo y seguro.

Si bien el proyecto se centró en la ejecución local, también se incluyeron parámetros de configuración para una **red pública**, específicamente **Polygon**, utilizando **HDWalletProvider** y una frase mnemónica almacenada en un archivo seguro. Esta configuración opcional fue diseñada con el objetivo de dejar abierta la posibilidad de escalar la solución a una red descentralizada de mayor alcance, en caso de que se requiriera en fases posteriores. Aunque esta conexión no se utilizó en la práctica dentro de este trabajo, su inclusión refleja la intención de proyectar el sistema hacia escenarios reales de uso, donde la verificación de documentos académicos pueda realizarse en una blockchain accesible de manera global.

El archivo de configuración también contempló aspectos relativos al **compilador de Solidity**, especificando la versión adecuada y habilitando opciones de optimización. Este ajuste resultó fundamental para asegurar la compatibilidad de los contratos con la red de destino y, al mismo tiempo, reducir el consumo de *gas* en caso de futuras implementaciones en un entorno

público. De este modo, se garantizó que el código desarrollado no solo funcionara en condiciones locales de prueba, sino que estuviera preparado para un posible despliegue en redes más amplias.

4.5. Análisis de Riesgos y Situaciones

El desarrollo del sistema permitió demostrar la viabilidad de emplear blockchain e IPFS para la autenticación de documentos académicos, sin embargo, también evidenció una serie de riesgos y limitaciones que deben considerarse en un posible escenario de implementación real dentro de la Universidad Francisco José de Caldas. Estos aspectos no invalidan el aporte del prototipo, pero sí marcan las fronteras y desafíos que deberán ser atendidos en fases posteriores.

En primer lugar, desde el punto de vista **técnico**, el uso de una blockchain local ofrece un entorno seguro y controlado, pero no refleja por completo la complejidad de un sistema desplegado a gran escala. La simulación con Ganache permitió registrar y verificar documentos de forma ágil, aunque resulta evidente que, en un escenario con miles de certificados, sería necesario optimizar la infraestructura o migrar a una red con mayor capacidad. De igual forma, la dependencia de IPFS introduce el riesgo de disponibilidad: mientras los archivos estén activos en la red, su recuperación es inmediata, pero si los nodos que alojan la información dejan de estar disponibles, los tiempos de respuesta podrían aumentar de manera considerable.

Un segundo conjunto de riesgos se encuentra en el ámbito **legal y normativo**. En Colombia, el marco regulatorio alrededor de blockchain aún se encuentra en construcción, lo que plantea interrogantes sobre la validez jurídica de un diploma registrado en una cadena de bloques. Aunque el sistema garantiza inmutabilidad y transparencia, su reconocimiento oficial dependerá de la evolución de la normativa educativa y tecnológica del país. Además, el tratamiento de datos personales asociado a la subida de documentos debe cumplir de manera estricta con la Ley de Habeas Data, evitando cualquier exposición indebida de información sensible.

También es necesario destacar los riesgos de tipo **organizacional y cultural**. La introducción de un sistema innovador como este requiere no solo de la infraestructura técnica, sino también de la capacitación de funcionarios y administrativos que gestionan los procesos

académicos. Es probable que se presente resistencia al cambio, ya que muchos de los actores están acostumbrados a la verificación manual o a sistemas más tradicionales. Esta barrera de adopción es tan relevante como las cuestiones técnicas, puesto que sin la aceptación institucional difícilmente se podrá consolidar la solución.

Finalmente, se reconocen las **limitaciones propias del prototipo**. El sistema fue validado únicamente en un entorno local, sin interacción con redes públicas o con los sistemas de gestión ya existentes en la universidad. Otro aspecto a tener en cuenta es que el sistema no contempla aún un manejo exhaustivo de roles más complejos, como validadores externos o empleadores, lo que restringe las pruebas a un círculo de interacción básico entre estudiantes y administradores.

Tabla 15:Análisis de Riesgos y Estrategias de Mitigación

Riesgo identificado	Impacto potencial	Estrategia de mitigación
Escalabilidad de la blockchain local	Saturación del sistema con múltiples transacciones simultáneas; lentitud en la verificación de documentos.	Migrar a una red de mayor capacidad (ej. Polygon, Ethereum testnet) y aplicar optimizaciones en los contratos inteligentes.
Disponibilidad de archivos en IPFS	Riesgo de que los documentos no estén siempre accesibles si los nodos que los almacenan dejan de estar activos.	Configurar un nodo institucional de IPFS en la universidad y usar servicios externos como Pinata o Filebase para redundancia.
Reconocimiento legal limitado	La validez de los certificados registrados en blockchain puede no ser aceptada formalmente por instituciones externas.	Trabajar en conjunto con las autoridades universitarias y regulatorias para adaptar el sistema a la normativa vigente.
Protección de datos personales	Posible exposición indebida de información sensible de estudiantes en el proceso de subida.	Cumplimiento estricto de la Ley de Habeas Data; anonimizar información y almacenar únicamente hashes en blockchain.
Resistencia al cambio organizacional	Funcionarios y usuarios pueden preferir procesos manuales, afectando la adopción del sistema.	Capacitación y talleres de sensibilización; demostrar beneficios prácticos como rapidez y seguridad.

Integración con sistemas institucionales	El prototipo no se conecta con plataformas actuales (SIAR, SAP), limitando su uso real.	Diseñar APIs o módulos de integración progresiva para conectar el sistema con las plataformas existentes.
Limitaciones del prototipo local	El sistema no contempla validadores externos (ej. empleadores) y se probó solo en entorno controlado.	Planear una fase piloto con usuarios externos, incluyendo pruebas en redes públicas para validar su alcance.

Anexo 2: Manual de Uso

La aplicación permite almacenar, consultar y verificar documentos académicos utilizando **blockchain** y **IPFS**. Todo se ejecuta en un entorno local, garantizando privacidad y control total sobre los datos. La interfaz fue diseñada en **React**, ofreciendo una experiencia fluida y clara para los usuarios.

5.1.1. Interfaz principal

Al abrir la aplicación, se observa un **panel limpio y organizado**, con dos opciones principales en el menú superior, que se muestran en la ilustración [10]:

Ilustración 10: Visual Botones Principales



Fuente: Elaboración propia

La interfaz principal de la aplicación presenta un diseño limpio y organizado, en el que destacan dos funciones principales: subir documentos y buscarlos. En la parte superior se incluye información técnica como la cuenta activa y la dirección del contrato inteligente, lo que aporta transparencia en el funcionamiento sin ser un requisito para el uso cotidiano.

5.1.2. Subir Documentos

En la sección de **Subir Documentos** se encuentra un formulario interactivo que recopila los datos esenciales del estudiante y del archivo que se desea registrar. Entre los campos obligatorios se incluyen el nombre completo y el número de identificación, elementos que

garantizan la trazabilidad del documento hacia su propietario legítimo. Adicionalmente, el usuario debe especificar el tipo de documento —por ejemplo, diploma, matrícula o certificado académico— y seleccionar el programa académico correspondiente a través de una lista desplegable. Este procedimiento, incorpora validaciones automáticas que evitan el envío de formularios incompletos. De este modo, el sistema alerta inmediatamente si falta algún dato, lo que contribuye a la calidad y consistencia de la información almacenada.

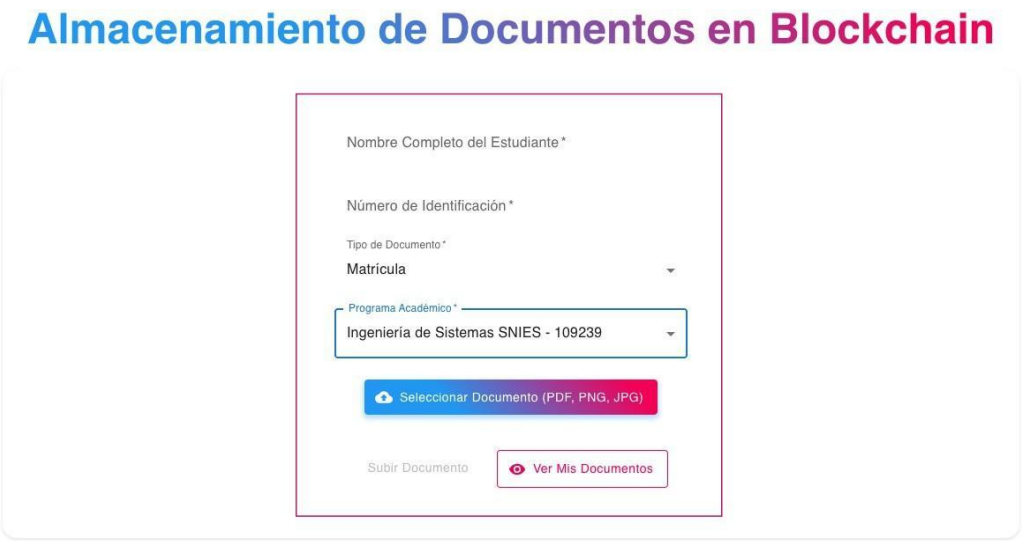
5.1.2.2 Selección de archivo:

Una vez completados los campos personales, el usuario puede proceder a la **selección del archivo**. El sistema admite formatos ampliamente utilizados como PDF, PNG y JPG, lo que garantiza compatibilidad con la mayoría de los documentos académicos digitales. En caso de que se intente cargar un archivo en un formato no permitido, la aplicación responde con un mensaje de error, reforzando la seguridad y estandarización del proceso. Tras esta validación, el archivo se envía a la red descentralizada de almacenamiento IPFS, que genera un identificador único o **CID**. Posteriormente, este CID es registrado en la blockchain mediante el contrato inteligente, vinculando así el archivo original con un registro inmutable y verificable.

5.1.2.3 Botones de acción:

La interfaz incluye además botones de acción que simplifican la interacción del usuario con el sistema. El primero de ellos, “Subir Documento”, ejecuta de manera automática el flujo completo: validación de campos, carga del archivo en IPFS y registro del CID en la blockchain. El segundo, “Ver Mis Documentos”, permite consultar de forma inmediata los archivos que el usuario ya ha registrado, presentando un resumen de su información básica como el tipo de documento, el programa académico y el hash correspondiente en IPF.

Ilustración 11: Componente Visual Cargar un Documento



Fuente: Elaboración propia

5.1.3. Listado de Documentos

El listado de documentos constituye un repositorio visual que organiza la información básica de cada archivo. Este incluye nombre, identificación, tipo de documento, programa académico y el identificador IPFS correspondiente. Asimismo, se ofrecen múltiples mecanismos de acceso —mediante gateways IPFS o exploradores de blockchain— y la posibilidad de verificación inmediata a través de códigos QR, lo que facilita la validación desde dispositivos móviles en distintos contextos de uso.

En síntesis, la sección de subida y listado de documentos articula en una misma interfaz la simplicidad de uso para el estudiante con la solidez técnica que aporta la combinación de IPFS y blockchain. Con ello, se logra un equilibrio entre usabilidad y seguridad, garantizando que los documentos académicos puedan ser registrados, consultados y compartidos con plena confianza.

Ilustración 12: Visualización Documentos Cargados



Fuente: Elaboración propia

5.1.4. Búsqueda de documentos

La sección de **Búsqueda de Documentos** se diseñó pensando en la agilidad y transparencia que requiere la validación académica. Su objetivo principal es permitir que cualquier persona pueda acceder, de manera rápida y confiable, a los certificados previamente registrados en el sistema.

El procedimiento inicia con el ingreso del número de identificación del estudiante, el cual actúa como llave de acceso a su historial documental. Con este dato, el sistema consulta los registros correspondientes y presenta los resultados en un listado organizado, lo que facilita la revisión de los documentos disponibles sin necesidad de realizar pasos adicionales.

Cada registro incluye la información esencial del archivo, como su tipo y fecha de registro, además de herramientas de acceso directo que agilizan el proceso de verificación. Entre estas opciones se destaca el uso de códigos QR: al seleccionarlos, el sistema despliega un modal con el código correspondiente, que puede ser escaneado desde un dispositivo móvil para acceder de inmediato al documento. Esta característica elimina la complejidad de manejar cadenas

alfanuméricas largas, ofreciendo en su lugar una experiencia sencilla y accesible para cualquier usuario.

En términos prácticos, esta funcionalidad resulta de gran valor en contextos donde el tiempo es un factor determinante. Un empleador, por ejemplo, puede validar la autenticidad de un diploma en cuestión de segundos, mientras que un área administrativa de otra institución académica puede corroborar certificados sin depender de procesos manuales. De esta forma, la búsqueda no solo cumple con un rol técnico, sino que también aporta eficiencia y confianza en escenarios reales de uso.

Ilustración 13: Visual Busqueda de Documento



5.1.5. Ejemplo de Uso

Como escenario de prueba, al consultar el número de identificación “12345”, el sistema devuelve un documento de tipo “Diploma” correspondiente al programa de Tecnología en Electrónica Industrial. Este resultado puede verificarse mediante los enlaces proporcionados o mediante el código QR generado, comprobando su autenticidad con la tecnología blockchain.

Ilustración 14: CODIGO QR - ID DOCUMENTO



Recomendaciones

Se le recomienda al usuario completar todos los campos para poder tener éxito en el proceso de la carga de documentos, así mismo se debería tener una copia local de los documentos originales. En cuanto lo visualizado, se debe verificar los enlaces y códigos QR antes de compartir cualquier documento. Y por último si el usuario desea realizar una búsqueda, el número de identificación es la manera de acceder más rápidamente.

Conclusiones

En primer lugar, el desarrollo de este proyecto demostró que la implementación de un sistema de autenticación de documentos basado en blockchain constituye una alternativa viable para reforzar la confiabilidad y la seguridad en el manejo de información académica. Aun cuando el entorno de ejecución fue local y controlado, se logró simular un flujo de trabajo completo que incluyó la carga de archivos, la generación de identificadores únicos mediante IPFS y la verificación de autenticidad a través de contratos inteligentes. Este ejercicio permitió comprobar que la tecnología blockchain puede transformar procesos tradicionalmente manuales y burocráticos en procedimientos más eficientes, trazables y resistentes a fraudes.

En segundo lugar, se evidenció la relevancia de un diseño de roles bien definido dentro del sistema. La diferenciación entre estudiantes y administradores permitió establecer un marco de responsabilidades claro, en el que cada actor ejecuta funciones específicas sin interferir en las de los demás. Este esquema, además de favorecer la organización interna, refuerza la confianza en el sistema al garantizar que las interacciones con la blockchain estén reguladas y se mantenga la integridad de la información académica.

Asimismo, la experiencia práctica puso en evidencia una serie de retos técnicos que resultan fundamentales para futuras implementaciones a mayor escala. Entre ellos destacan la necesidad de optimizar los tiempos de respuesta en las verificaciones, mejorar la eficiencia en la gestión de datos almacenados en blockchain y prever la escalabilidad del sistema en escenarios con un volumen considerable de usuarios y documentos. Estas limitaciones, lejos de restar valor al proyecto, representan oportunidades de mejora que permiten orientar investigaciones posteriores hacia soluciones más robustas y aplicables en entornos reales.

Finalmente, se concluye que este proyecto no solo aporta una solución tecnológica funcional, sino que también introduce una visión innovadora para la gestión documental en instituciones académicas. La integración de blockchain con IPFS mostró ser una estrategia efectiva para garantizar seguridad, transparencia y confiabilidad en el registro de certificados. Aunque se trata de una implementación inicial, los resultados obtenidos sientan las bases para

que universidades como la Distrital Francisco José de Caldas avancen hacia sistemas digitales modernos, contribuyendo así a la transformación de sus procesos administrativos y académicos.

Bibliografía

[1] T. W. I. Keilitz, "Blockchain and international development: Can blockchain technology be the solution to effective land registration systems in developing nations," *William & Mary Policy Review*, 2018.

[2] D. L. Anning, "https://cwas.uestc.edu.cn/," Apr. 8, 2025. [En línea]. Disponible en: https://cwas.uestc.edu.cn/info/1042/3558.htm. [Accedido: Jun. 14, 2025].

[3] J. Porxas y C. J. Porxas, Blockchain: Seguridad y confianza para la gestión digital. Universidad de Alicante, 2018.

[4] U. EAN, "Somos la primera universidad colombiana en emitir títulos con tecnología blockchain," Jan. 25, 2019. [En línea]. Disponible en: https://universidadean.edu.co. [Accedido: Jun. 15, 2025]

[5] T. Signe, "Casos de éxito: Instituciones educativas que emiten diplomas en Blockchain en Colombia," Oct. 8, 2023. [En línea]. Disponible en: https://www.thomas-signe.co. [Accedido: Jun. 14, 2025].

[6] A. d. N. UNAL, "La UNAL entra en la era de diplomas con tecnología blockchain," May 31, 2019. [En línea]. [Accedido: Jun. 14, 2025].

[7] blockcerts.org, "Blockcerts from MIT Media Lab," 2018. [En línea]. Disponible en: https://www.researchgate.net. [Accedido: 2025].

[8] S. D.-G. Guida, "Decreto 2364 de 2012," Nov. 22, 2012. [En línea]. [Accedido: Jun. 10, 2025].

[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [En línea]. Disponible en: https://bitcoin.org/bitcoin.pdf.

[10] M. M. L. L. Initiative, "Blockcerts — An Open Infrastructure for Academic Credentials on the Blockchain," Oct. 24, 2016. [En línea]. [Accedido: May 8, 2025].

[11] H. B. T. F. Business, "Introduction to Hyperledger Business Blockchain," Aug. 2, 2017. [En línea]. [Accedido: May 8, 2025].

[12] H. Fabric, "Architecture Explained," 2018. [En línea]. [Accedido: 2025].

[13] Hyperledger, "Hyperledger-fabricdocs Documentation," Sep. 28, 2021. [En línea]. [Accedido: Jun. 13, 2025].

[14] I. Fetsyak, "Contratos inteligentes: Análisis jurídico desde el marco legal español," Dec. 14, 2020. [En línea]. [Accedido: Jun. 13, 2025].

[15] Arxiv, "IPFS - Content Addressed, Versioned, P2P File System," Jul. 14, 2014. [En línea]. [Accedido: Jun. 14, 2025].

[16] W3C, "Verifiable Credentials Data Model v2.0," May 14, 2025. [En línea]. [Accedido: Jun. 14, 2025].

[17] AWS, "¿Qué es la tecnología de cadena de bloques?," [En línea]. [Accedido: Jun. 14, 2025].

[18] StartNet, "What is decentralization in blockchain?," Feb. 26, 2025. [En línea]. [Accedido: Jun. 14, 2025].

[19] GeeksforGeeks, "Immutability in Blockchain," 2025. [En línea]. [Accedido: Jun. 14, 2025].

[20] F. PBC, "Blockchain Immutability — Why Does it Matter?," 2025. [En línea]. [Accedido: Jun. 14, 2025].

[21] S. Directory, "Blockchain Transparency Term," 2025. [En línea]. [Accedido: Jun. 14, 2025].

[22] IBM, "What is blockchain security?," 2025. [En línea]. [Accedido: 2025].

[23] Investopedia, "What Are Consensus Mechanisms in Blockchain and Cryptocurrency?," 2018. [En línea]. [Accedido: 2025].

[24] IBM, "What are Smart Contracts on Blockchain?," 2025. [En línea]. [Accedido: 2025].

[25] PMC, "Blockchain and Higher Education Diplomas," Feb. 18, 2021. [En línea]. [Accedido: Jun. 14, 2025].

[26] Openaccess UOC, "Content Management in Blockchain," 2025. [En línea]. [Accedido: Jun. 14, 2025].

[27] I. Logunova y B. O. Logunova, "Scalability and interoperability in blockchain," Serokell, Sep. 2024. [En línea]. [Accedido: Jun. 16, 2025].

[28] Reuters, "What is tokenization and is it crypto's next big thing?," Jul. 2023. [En línea]. [Accedido: Aug. 14, 2025].

[29] Exodus, "How do consensus mechanisms like PoW and PoS work?," May 25, 2025. [En línea]. [Accedido: Jun. 19, 2025].

[30] Rapidinnovation, "Blockchain Consensus Mechanisms Explained: PoW vs PoS," Sep. 18, 2025. [En línea]. [Accedido: 2025].

[31] Wikipedia, "Prueba de autoridad," Sep. 27, 2024. [En línea]. [Accedido: 2025].

[32] N. T. M. Bello, "Evaluación del programa de gestión documental para la Universidad Distrital," 2023. [En línea]. [Accedido: 2025].

[33] Universidad Distrital Francisco José de Caldas, "Archivística y Gestión de la Información Digital," 2025. [En línea]. [Accedido: 2025].

[34] S. E. Moscoso Urdaneta, "Certificación digital de documentos," Dec. 13, 2019. [En línea]. [Accedido: Jun. 16, 2025].

[35] MinTIC, "Guía de referencia de Blockchain," Dec. 2020. [En línea]. [Accedido: Jun. 2025].