Logotipo

El contenido generado por IA puede ser incorrecto.

Universidad Central del Ecuador

Facultad de Ingeniería y Ciencias Aplicadas

Carrera de Ingeniería Informática

**Prototipo de aplicación para la certificación de documentos digitales en instituciones de educación superior basado en la tecnología Blockchain.**

Trabajo de titulación – Opción: Proyecto de investigación presentado para obtener el grado académico de Ingeniero en Informática.

Autores: Henry Paolo Felicita Vasco

Tutor: Ing. Santiago Morales Cardoso. PhD

Quito – 2024

https://licensebuttons.net/l/by-nc-sa/3.0/88x31.png

# Índice general de contenidos

[Índice general de contenidos i](#_Toc190265334)

[Capítulo 1 1](#_Toc190265335)

[1. Generalidades 1](#_Toc190265336)

[1.1. Análisis del problema 1](#_Toc190265337)

[1.2. Antecedentes 1](#_Toc190265338)

[1.3. Planteamiento del problema 3](#_Toc190265339)

[1.4. Hipótesis y Justificación 4](#_Toc190265340)

[1.4.1. Hipótesis 4](#_Toc190265341)

[1.4.2. Justificación 4](#_Toc190265342)

[1.5. Objetivos 5](#_Toc190265343)

[1.5.1. General 5](#_Toc190265344)

[1.5.2. Específicos 5](#_Toc190265345)

[Capítulo 2 6](#_Toc190265346)

[2. MARCO TEÓRICO 6](#_Toc190265347)

[2.1. Conceptos 6](#_Toc190265348)

[2.1.1. Certificación 6](#_Toc190265349)

[2.1.2. Certificación Académica 6](#_Toc190265350)

[2.2. Blockchain 6](#_Toc190265351)

[2.2.1. Características de Blockchain 7](#_Toc190265352)

[2.2.2. Arquitectura de Blokchain 8](#_Toc190265353)

[2.2.3. Bloque 8](#_Toc190265354)

[2.2.4. Mecanismo de Consenso 10](#_Toc190265355)

[2.3. Smart Contracts 11](#_Toc190265356)

[2.3.1. Estructura de un Smart Contract 11](#_Toc190265357)

[2.3.2. Ethereum y EVM 12](#_Toc190265358)

[2.3.3. Solidity 13](#_Toc190265359)

[Capítulo 3 15](#_Toc190265360)

[3. Metodología experimental 15](#_Toc190265361)

[3.1. Metodologías de Desarrollo de Software 15](#_Toc190265362)

[3.2. Metodología Usada en la Investigación 15](#_Toc190265363)

[Cálculos y resultados 17](#_Toc190265364)

[Discusión de resultados 17](#_Toc190265365)

[Conclusiones 17](#_Toc190265366)

[Recomendaciones 17](#_Toc190265367)

[Referencias 17](#_Toc190265368)

[Anexos 17](#_Toc190265369)

# Capítulo 1

## Generalidades

### Análisis del problema

### Antecedentes

El desarrollo de nuevas tecnologías abre posibilidades para la creación de negocios innovadores y la optimización de los ya existentes. La cuarta revolución industrial, impulsada por internet, ha dado lugar a importantes avances tecnológicos que han transformado numerosos aspectos de la vida cotidiana, generando un notable impacto en la sociedad. La tecnología blockchain surge como una solución innovadora para abordar diversos problemas en distintas áreas como la salud, educación el gobierno entre otros. En el ámbito educativo, esta tecnología facilita la eliminación de cuellos de botella en diversos procesos y proporciona una mayor protección para la información dentro de las instituciones. [1]

Generalmente las instituciones educativas suelen gestionar grandes volúmenes de expedientes, los cuales son frecuentemente solicitados por los estudiantes para diversos fines, como la transferencia de créditos, la obtención de becas, seguros, cambio de carrera o el cumplimiento de requisitos para ingresar a nuevos programas académicos. Aunque la transferencia de expedientes académicos es una tarea común en el día a día de estas instituciones, a menudo implica costos significativos debido a que los procesos de transferencia y verificación son altamente manuales. [2]

Además, de los problemas asociados con la emisión de certificados académicos que amenazan la integridad de las instituciones educativas, incluso en las más prestigiosas, como el Instituto Tecnológico de Massachusetts. [3]

En ese sentido la tecnología blockchain podrían abordar tales retos a través del despliegue de una plataforma abierta, descentralizada, y directa, en donde se pueda des intermediar el flujo de información, logrando que se pueda mejorar la transparencia y la confianza en los registros educativos. [4]

**Aplicación de blockchain en el sector de la salud**

La tecnología blockchain se presenta como una herramienta muy prometedora para abordar el problema de la dispersión de la información médica de los pacientes cuando reciben atención en distintos centros de salud. En la actualidad, los datos médicos suelen estar fragmentados y carecen de un expediente único, lo que dificulta su acceso. Gracias a la blockchain, es posible recuperar de manera rápida y segura los registros médicos, garantizando la integridad y permanencia de la información relacionada con el diagnóstico y tratamiento de cada paciente. Todo lo que se refiere a exámenes, biopsias y procedimientos quedan almacenados en una red descentralizada, creando un historial médico inmutable que solo puede ser consultado con la autorización del paciente, lo cual es fundamental para el desarrollo de tratamientos personalizados. [5]

**Aplicación de blockchain en la cadena de suministros**

La gestión y distribución de medicamentos o productos farmacéuticos representa un desafío crucial tanto a nivel nacional como internacional. Existe el riesgo de que estos productos sean adulterados, etiquetados de manera fraudulenta o desviados desde su punto de origen con la intención de engañar a los consumidores, haciéndoles creer que están adquiriendo un producto auténtico. Asimismo, la cadena de suministro en el sector de la salud es un complejo sistema de negocios que abarca procesos como adquisición, producción, almacenamiento y distribución de productos y servicios médicos. Esta red incluye normas y procedimientos esenciales para garantizar el acceso a los medicamentos y satisfacer las necesidades de los pacientes, profesionales de la salud e instituciones médicas. En términos generales, la circulación de medicamentos falsificados o de baja calidad representa un riesgo significativo para los pacientes y sus familias. En este contexto, la tecnología blockchain surge como una solución innovadora para optimizar la transparencia, eficiencia y seguridad en la cadena de suministro. Al descentralizar el control de los datos y garantizar un registro inalterable de la información, esta tecnología permite eliminar intermediarios y establecer sistemas de seguimiento en tiempo real, ofreciendo mayor confianza a todos los actores involucrados en el proceso. [6]

### Planteamiento del problema

En las instituciones de educación superior, la certificación y validación de documentos académicos, como títulos, certificados y constancias, sigue dependiendo en gran medida de procesos manuales y centralizados, esto conlleva a posibles problemas como falsificaciones de documentos, demoras en la verificación de autenticidad y costos administrativos elevados. Adicionalmente, los egresados y empleadores enfrentan dificultades para validar credenciales en tiempo real, lo que impacta la eficiencia de procesos de contratación y admisión a estudios avanzados. Las soluciones basadas en correo electrónico, transferencia de registros PDF y portales de entregas seguros, para la verificación, validación o homologación de documentos en línea son cada vez más comunes, teniendo estas un enfoque más moderno, pero todavía existen limitaciones en términos de verificación y escalabilidad. [1]

La tecnología blockchain ha emergido como una alternativa viable para garantizar la autenticidad, inmutabilidad y trazabilidad de documentos digitales. Sin embargo, muchas universidades aún no han adoptado esta tecnología debido a la ausencia de soluciones prácticas y accesibles que faciliten su implementación.

En este contexto, surge la necesidad de desarrollar un prototipo de aplicación basado en blockchain que permita a las instituciones de educación superior certificar y verificar documentos digitales de manera segura, descentralizada y eficiente. Por esta razón este estudio busca analizar la viabilidad de dicha solución y evaluar su impacto en la reducción del fraude académico y la optimización de procesos administrativos en el ámbito educativo.

### Hipótesis y Justificación

#### Hipótesis

¿Es posible implementar un prototipo basado en Blockchain para la certificación de documentos digitales en instituciones de educación superior?

#### Justificación

En Ecuador, las instituciones educativas operan de manera independiente en cuanto a los sistemas de emisión y verificación de certificados, lo que significa que cada entidad gestiona de forma centralizada sus propios procesos. Como resultado, los estudiantes deben encargarse del almacenamiento de los certificados para integrarlos en su portafolio profesional. Estos sistemas centralizados aumentan la carga de trabajo en las instituciones, especialmente a la hora de verificar la autenticidad de los documentos, los cuales son vulnerables a falsificación.

El propósito de este proyecto es desarrollar una solución basada en la tecnología blockchain para optimizar la verificación, validación y homologación de los certificados de suficiencia en el idioma inglés en la Universidad Central del Ecuador. Esta implementación busca mejorar la eficiencia de los procesos administrativos, ofreciendo un sistema ágil, seguro y confiable.

La adopción de blockchain proporciona diversas ventajas dentro del ámbito educativo, tales como la reducción de intermediarios en la validación de documentos, la eliminación de cuellos de botella en los trámites administrativos y la disminución de los tiempos de espera. Además, garantiza la autenticidad e inmutabilidad de la información, fortaleciendo la confianza y transparencia en la certificación académica además de reducir riesgos como la falsificación o pérdida de documentos.

El impacto de esta propuesta no solo beneficiará a la Universidad Central del Ecuador, sino que también tiene como objetivo extenderse a otras instituciones de educación superior interesadas en modernizar sus procesos, transformando el sistema hacia entornos interconectados, abiertos y confiables, capaces de registrar de manera precisa el desempeño estudiantil y facilitar la transferencia de certificados, expedientes académicos y cualquier otra información relevante relacionada con la trayectoria universitaria de los estudiantes.

### Objetivos

#### General

Crear un prototipo de aplicación web utilizando tecnología blockchain para la certificación de la culminación de estudios del idioma inglés en el Instituto académico de Idiomas de la Universidad Central del Ecuador, garantizando la autenticidad, seguridad y transparencia en la validación de los certificados académicos.

#### Específicos

* Proponer un modelo de solución basado en blockchain para la validación de certificados de estudios del idioma inglés en el Instituto Académico de Idiomas de la Universidad Central del Ecuador.
* Identificar y seleccionar la herramienta tecnológica más adecuada para el desarrollo del prototipo.
* Aplicar una metodología ágil que permita mejorar la flexibilidad y eficiencia en el desarrollo del proyecto.
* Realizar una prueba piloto con 20 certificados académicos dentro del Instituto Académico de Idiomas para validar la efectividad del modelo propuesto.

# Capítulo 2

## MARCO TEÓRICO

### Conceptos

#### Certificación

El término certificación se define como la acción y efecto de certificar o el documento en que se asegura la verdad de un hecho. Es decir, es un documento emitido por una entidad competente que confirma la autenticidad de algo. La certificación se materializa en un certificado, que puede ser de distintos tipos, como certificación de empresas, productos y personas. [7]

#### Certificación Académica

Es un documento oficial que acredita el historial académico de una persona. Generalmente, es emitido por una institución educativa (como una universidad) y contiene información detallada sobre los estudios realizados por el estudiante, incluyendo las asignaturas cursadas, las calificaciones obtenidas, las fechas de asistencia y la titulación alcanzada.

Este tipo de certificación es útil cuando un estudiante o egresado necesita demostrar su formación académica para trámites laborales, admisiones a otros programas educativos, convalidaciones de estudios en el extranjero o solicitudes de becas, entre otros. [1]

### Blockchain

El término *Blockchain*, también conocido como *cadena de bloques*, es una tecnología considerada disruptiva que evoluciona constantemente y es utilizada por diversas empresas para aprovechar sus características. Se considera una de las principales tecnologías de la cuarta revolución industrial. [8]

Blockchain es una red compuesta por varios nodos que contienen registros almacenados en cadenas de bloques. Funciona como una base de datos distribuida en la que la información se organiza en bloques, y cada bloque está vinculado al anterior mediante criptografía, formando una cadena. Esta cadena se replica en cada nodo de la red, garantizando disponibilidad y seguridad. [9]

Esta tecnología elimina la necesidad de un tercero como verificador, ya que la red misma verifica y valida las transacciones, haciendo que sea extremadamente difícil alterar o modificar la información sin que el resto de la red lo detecte. [10]

#### Características de Blockchain

A continuación, se presentan algunas propiedades que distinguen a esta tecnología.

1. **Descentralización:** La información dentro de una blockchain se distribuye entre múltiples nodos en la red, evitando que una sola entidad tenga control absoluto sobre los registros. Esto minimiza el riesgo de manipulación y fallos del sistema. [11]
2. **Inmutabilidad:** Una de las características esenciales de blockchain es que la información se registra en bloques enlazados criptográficamente. Una vez añadido un bloque a la cadena, no puede ser alterado ni eliminado, garantizando así la seguridad e integridad de los datos almacenados. [11]
3. **Disponibilidad:** Dado que la cadena de bloques está replicada en múltiples nodos, la información es accesible en todo momento. Esto garantiza una alta disponibilidad, ya que las transacciones no dependen de un único servidor. [12]
4. **Transparencia:** En una blockchain pública, todos los participantes pueden visualizar las transacciones registradas, lo que permite su verificación y auditoría. Esta cualidad fortalece la confianza en la red, ya que cualquiera puede revisar el historial de operaciones. [1]
5. **Anonimato y privacidad:** A pesar de la transparencia de las blockchain públicas, los usuarios pueden preservar su identidad mediante direcciones alfanuméricas en lugar de nombres reales. En el caso de blockchain privadas, es posible ajustar los niveles de anonimato y control de acceso para una mayor protección en las transacciones. [9]

#### Arquitectura de Blokchain

Una cadena de bloques es una secuencia de bloques que almacena un historial completo de todas las transacciones en un libro contable descentralizado y público.

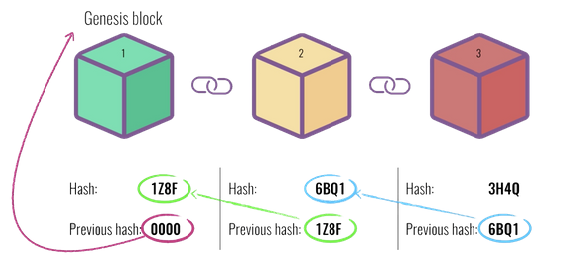


Fig. 1. Estructura blockchain

Nota: Álvaro Santos García [13]

La figura 1 ilustra un ejemplo de una cadena de bloques. Cada bloque está vinculado al anterior mediante un hash criptográfico, en un bloque solo puede existe un bloque padre, el único bloque que no contiene un bloque padre es el primer bloque de la cadena también conocido como bloque génesis. [13]

#### Bloque

Un bloque es un registro público que agrupa un conjunto de transacciones verificadas y distribuidas en todos los nodos que conforman una cadena de bloques. [8]

Diagrama, Texto

El contenido generado por IA puede ser incorrecto.

Fig. 2. Estructura de un bloque

Nota: Carlos Reyes Sánchez [8]

Como muestra la figura 2, la estructura general de un bloque dentro de una blockchain, el cual se compone de dos partes principales: el encabezado y el cuerpo.

El encabezado del bloque contiene metadatos esenciales, como:

1. La *versión del bloque*, que define las reglas de validación que deben aplicarse.
2. Una *marca de tiempo (timestamp),* que registra el momento exacto en el que se creó el bloque.
3. El *tamaño del bloque*, medido en bits, que establece el límite para considerar válido un hash.
4. El *nonce*, un número entero que comienza en cero y aumenta progresivamente con cada intento de resolución del problema criptográfico asociado a la creación del bloque.
5. El *hash del bloque padre*, un valor de 256 bits que enlaza con el bloque anterior, excepto en el caso del bloque génesis.
6. La *raíz del árbol de Merkle*, una estructura de datos que almacena hashes criptográficos organizados de manera jerárquica, facilitando la verificación eficiente de la integridad de grandes volúmenes de información. [8]

Por otro lado, el cuerpo del bloque almacena las transacciones validadas, asegurando la integridad y la inmutabilidad de los datos dentro de la cadena. [12]

Gracias a la estructura del árbol de Merkle, la seguridad de las transacciones dentro de un bloque está garantizado, ya que cualquier alteración en los datos provocaría un cambio en la raíz de Merkle, afectando la cadena de hashes y, en consecuencia, invalidando la autenticidad del bloque. [13]

#### Mecanismo de Consenso

En términos generales, los mecanismos de consenso, también conocidos como algoritmos o protocolos de consenso, se refieren a un conjunto de reglas que regulan el flujo de información dentro de una blockchain. Constituyen en el fundamento de cualquier blockchain, ya que determinan quién y cómo se genera un nuevo bloque en la cadena. Existen diversos tipos de mecanismos de consenso, algunos de los más relevantes se describen a continuación. [14]

1. **Prueba de trabajo (PoW - Proof of Work):** Este mecanismo se basa en la resolución de un problema matemático complejo que requiere un alto poder computacional para validar y agregar un nuevo bloque a la blockchain. [11]
2. **Prueba de participación (PoS - Proof of Stake):** En este modelo, la probabilidad de que un usuario genere el próximo bloque está determinada por la cantidad de monedas que posee. A mayor participación en la red, menor es la posibilidad de que un usuario actúe de manera maliciosa. [12]
3. **Prueba de participación delegada (DPoS - Delegated Proof of Stake):** En este enfoque, los participantes de la red seleccionan delegados responsables de validar y añadir nuevos bloques a la cadena. [11]

Cualquier mecanismo de consenso debe cumplir con tres principios fundamentales:

1. *Validez*, garantizando que solo las transacciones legítimas sean aprobadas por nodos autorizados.
2. *Conformidad,* asegurando que todos los nodos honestos lleguen a un acuerdo sobre el estado de la red.
3. *Terminación*, permitiendo que todos los nodos legítimos alcancen una decisión definitiva.

Además, estos algoritmos deben incluir mecanismos de seguridad para proteger la blockchain contra ataques y eventos adversos. [11]

### Smart Contracts

La aparición de la tecnología blockchain en la segunda generación demostró que podía usarse más allá de realizar simples pagos, transacciones y transferencias que involucran a sistemas financieros, por tanto, surgen los contratos inteligentes. Esta tecnología se lo puede definir como un programa que contiene un conjunto de instrucciones que se ejecutan de forma automática en cada nodo presente en la red en función del cumplimiento de las condiciones específicas del código. Esto crea confianza entre dos partes que no se conocen entre sí, ya que el código se ejecuta públicamente en la red y es verificable. [4]

#### Estructura de un Smart Contracto

Un contrato inteligente se compone de los siguientes elementos:

1. *Dirección*: Es un identificador único dentro de la blockchain.
2. *Valor*: Representa la cantidad de criptomoneda asociada al contrato.
3. *Funciones*: Son instrucciones programadas que se pueden ejecutar dentro del contrato.
4. *Estado*: Son los datos almacenados, los cuales pueden modificarse dependiendo de la ejecución de las funciones.

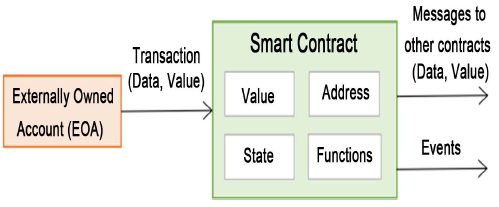


Fig. 3. Estructura de un contrato inteligente

Nota: Bhabendu Kumar [16]

Como se indica en la figura 3 se presenta un ejemplo simple de un contrato inteligente. Este contrato recibe la transacción como entrada, ejecuta el código pertinente y activa los eventos de salida. Según la lógica implementada en la función, los estados del contrato cambian durante su ejecución [15]

#### Ethereum y EVM

Ethereum es una plataforma digital creada en 2015 por Vitalik Buterin que se basa en la tecnología blockchain introducida por Bitcoin. Aunque su estructura es similar a la de Bitcoin, Ethereum incorpora un lenguaje de programación que permite a los desarrolladores diseñar software capaz de gestionar transacciones y automatizar procesos mediante contratos inteligentes. [16]

Esta plataforma es de código abierto, lo que significa que cualquier programador puede acceder a su estructura, modificarla y mejorarla, además de desarrollar aplicaciones sobre ella gracias a la Máquina Virtual de Ethereum (EVM). [17]

La EVM es un entorno de ejecución que opera dentro de la red Ethereum sin depender del lenguaje de programación utilizado. Su propósito es facilitar y optimizar la creación de aplicaciones en la blockchain, ya que admite un lenguaje de programación Turing Completo. En otras palabras, significa que el lenguaje posee la capacidad para que un ordenador pueda resolver operaciones computacionales en un determinado tiempo y con los recursos disponibles. [4]

#### Solidity

Existen diferentes lenguajes de programación utilizados para desarrollar contratos inteligentes. En esta investigación, nos centraremos en uno de los más populares y respaldados: Solidity. Este lenguaje de alto nivel permite a los desarrolladores crear bloques de código que agrupan datos y funciones, los cuales se convierten en contratos inteligentes dentro de la red blockchain de Ethereum. Solidity fue diseñado con el objetivo de asegurar que los contratos inteligentes se ejecuten de manera eficiente y correcta en cualquier plataforma que sea compatible con la Ethereum Virtual Machine (EVM). [12]

Entre las características más destacadas de Solidity están:

1. **Orientación a objetos**: Solidity sigue los principios de la programación orientada a objetos, utilizando clases para crear objetos que interactúan entre sí. Esto facilita la creación de código reutilizable y fácil de mantener. [18]
2. **Aprendizaje accesible**: La sintaxis de Solidity es similar a la de JavaScript, lo que facilita su aprendizaje para desarrolladores que ya tienen experiencia con JavaScript o con otros lenguajes backend como Java o .NET. Además, el lenguaje cuenta con una documentación bastante completa, y se requiere solo un conocimiento básico del entorno para comenzar a trabajar con él. [19]
3. **Optimización para la EVM**: Solidity está específicamente diseñado para Ethereum y su Ethereum Virtual Machine (EVM). Su propósito es ofrecer una forma sencilla y eficiente de desarrollar contratos inteligentes que aprovechen al máximo las capacidades de la EVM. [18]

# Capítulo 3

## Metodología experimental

La metodología es un componente fundamental dentro del proceso de desarrollo de una investigación, según la Real Academia Española la define como la ciencia del método, es decir, el conjunto de procedimientos que se siguen en una investigación científica o en una exposición doctrinal [20]. En este sentido, el término “método” hace referencia a la ruta a seguir a través de un conjunto de pasos, normas y procedimientos previamente establecidos, aplicados de forma consciente y deliberada, con el propósito de alcanzar un determinado fin que puede ser tangible o conceptual [21].

Según Fidias [22], la metodología de investigación aplicada tiene como propósito la producción de nuevos conocimientos con aplicación inmediata a la solución de problemas prácticos. Esta se fundamenta principalmente en los hallazgos tecnológicos de la investigación básica, desempeñando un papel clave en la unión entre la teoría y el producto. Por su parte Lozada [23], señala que este tipo de investigación puede arrojar dos clases de resultados: el primero corresponde al núcleo tecnológico, que engloba el conocimiento general requerido para desarrollar un producto; mientras que el segundo se relaciona con la tecnología específica, donde se materializa un producto o una de sus partes con un valor añadido.

Tomando en cuenta estas consideraciones, se ha decidido emplear esta metodología, ya que se pretende desarrollar un prototipo para la certificación de la culminación de estudios del idioma inglés en el Instituto académico de Idiomas de la Universidad Central del Ecuador. Esta elección permitirá establecer una ruta clara y detallada para el proyecto, facilitando la creación de una solución efectiva y asegurando el cumplimiento de los objetivos planteados.

Por lo tanto, se propone una serie de pasos a seguir para el desarrollo del presente trabajo.

**Propuesta del prototipo:** El primer paso es definir con precisión la funcionalidad que tendrá el prototipo de aplicación. Para comprender el alcance del proyecto, se decidió llevar a cabo una serie de entrevistas con el propósito de conocer el proceso de certificación académica dentro del Instituto Académico de Idiomas. A través de estas, se identificará qué áreas y personas intervienen en dicho proceso, lo que permitirá determinar los requisitos, funcionalidades y características que deberá cumplir el contrato inteligente, así como elaborar el diagrama del modelo con base en la información proporcionada por las partes interesadas.

**Descripción de la arquitectura:** El siguiente paso consiste en llevar a cabo un análisis exhaustivo de las funcionalidades del contrato inteligente para definir los requerimientos de la arquitectura y el entorno de desarrollo. Esto permitirá tener una visión clara de la correcta preparación del entorno de trabajo.

**Selección de herramientas:** Una vez definidos los requerimientos para el desarrollo del proyecto, el siguiente paso es seleccionar un conjunto de herramientas, preferiblemente de software libre, que respalden la arquitectura y el entorno de desarrollo establecidos en la fase inicial.

**Desarrollo del prototipo propuesto:** Con la arquitectura y el entorno de trabajo establecidos, lo siguiente es la creación de los contratos inteligentes, por tanto, esta fase se centrará en la codificación, detallando minuciosamente cada uno de sus componentes. Al final, se describirá el proceso de configuración, así como los pasos necesarios para compilar y desplegar el contrato inteligente en la red de pruebas.

**Interacción con el contrato inteligente:** En la fase final, se llevará a cabo la interacción con los contratos inteligentes mediante una interfaz gráfica, permitiendo su implementación en la red de pruebas. En este apartado, se explicará el desarrollo de la interfaz, sus componentes y la forma en que los usuarios deberán utilizarla para garantizar la validez del certificado generado.

# Cálculos y resultados

# Discusión de resultados

# Conclusiones

# Recomendaciones

# Referencias

# Anexos