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

**Cesión de derechos de autor.**

1. **Cesión de derechos de autor.**

Mediante el envío del presente correo electrónico ACEPTO EN FORMA EXPRESA en calidad de autor, titular de los derechos morales y patrimoniales del trabajo de titulación: ***Prototipo de aplicación para la certificación de documentos digitales en instituciones de educación superior basado en la tecnología blockchain***. De conformidad con el Artículo 114 del **Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación**:

“De los titulares de derechos de obras creadas en las instituciones de educación superior y centros educativos.- En el caso de las obras creadas en centros educativos, universidades, escuelas politécnicas, institutos superiores técnicos, tecnológicos, pedagógicos, de artes y los conservatorios superiores, e institutos públicos de investigación como resultado de su actividad académica o de investigación tales como trabajos de titulación, proyectos de investigación o innovación, artículos académicos, u otros análogos, sin perjuicio de que pueda existir relación de dependencia, la titularidad de los derechos patrimoniales corresponderá a los autores. Sin embargo, el establecimiento tendrá una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra con fines académicos.”

Asimismo, autorizo a la Universidad Central del Ecuador para que realice la publicación de este trabajo de titulación en el repositorio institucional en formato digital tal como lo establece el documento RHCU.SO.22 CIRCULAR No. 027-2021 del 11 de junio del año 2021 con nombre “Creación del archivo digital de la Universidad Central del Ecuador”, y de conformidad a lo dispuesto en el Artículo 144 de la **Ley Orgánica de Educación Superior**:

“Trabajos de Titulación en formato digital. - Todas las instituciones de educación superior estarán obligadas a entregar los trabajos de titulación que se elaboren para la obtención de títulos académicos de grado y posgrado en formato digital para ser integradas al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.”

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

El autor reconoce que este mensaje electrónico de aceptación reemplaza a mi firma física, y tiene la validez legal de conformidad a lo dispuesto en la **Ley de Comercio Electrónico, Firmas y Mensajes de Datos**, en sus artículos 3, 6 y 8,

**“Art. 3.-** Incorporación por remisión. - Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.”

**“Art. 6.-** Información escrita. - Cuando la Ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que éste contenga sea accesible para su posterior consulta.”

**“Art. 8.-** Conservación de los mensajes de datos. - Toda información sometida a esta Ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones:

1. Que la información que contenga sea accesible para su posterior consulta;
2. Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;
3. Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,
4. Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.”

(Este documento esta validado por el autor a través del formato en el archivo de Mensaje de datos con descripción: “DERECHOS DE AUTOR”)

**Henry Paolo Felicita Vasco**

**1723166532**

**Dedicatoria.**

Dedico este trabajo con todo mi corazón a mi madre, María Soledad Vasco, por ser mi pilar más firme, por su amor incondicional, su ejemplo de vida y el constante apoyo que me ha brindado en cada paso de este camino. Su fortaleza y entrega han sido mi mayor fuente de inspiración.

Extiendo esta dedicatoria a mi esposa, Yahira Michell Andrade, por su amor, comprensión y compañía inquebrantable en los momentos más difíciles. Su presencia y aliento me han dado la fuerza necesaria para seguir adelante y superar cada desafío.

Con profundo amor y gratitud, también dedico este logro a la memoria de mi abuelita, María Mercedes Chasipanta (1932–2009), quien me inculcó principios de ética y humildad, me enseñó a caminar siempre por el sendero correcto, y me mostró que el sacrificio y la constancia son las claves para alcanzar nuestros sueños.

**Agradecimiento.**

En primer lugar, deseo expresar mi más profundo agradecimiento a mis padres, Pedro y Soledad, por ser un pilar fundamental en cada etapa de mi formación, desde el inicio de mi camino como estudiante hasta la culminación de mi carrera universitaria, siempre estuvieron presentes, brindándome todo su apoyo, guiándome con sabiduría, escuchándome con paciencia y rodeándome con su amor incondicional para alcanzar mis objetivos, espero que todo el tiempo hayan sentido cuanto los valoro, respeto y admiro.

A mi esposa, Yahira, gracias por caminar conmigo en este largo trayecto, tu presencia constante, tu preocupación diaria y tu apoyo incondicional han sido fundamentales en todo momento, especialmente durante la elaboración de esta tesis, gracias por ser parte de cada paso y por acompañarme con tanto amor.

Extiendo también mi agradecimiento a mis hermanos, sobrinos y tíos, cuyas palabras de aliento y muestras de ánimo me han dado fuerza. Gracias a ustedes, estos últimos meses han sido más llevaderos y llenos de motivación. Su compañía ha sido fundamental en el cierre de una etapa más en mi vida.

Finalmente, quiero expresar mi sincero agradecimiento al Ing. Santiago Morales Cardoso, PhD, por su valiosa guía, dedicación y compromiso, no solo en el desarrollo de este trabajo, sino también por su labor como docente, siempre transmitiendo un conocimiento claro, sólido y enriquecedor, sus consejos han sido de gran ayuda tanto en el ámbito académico como en lo personal.

**Resumen.**

Las instituciones de educación superior enfrentan desafíos significativos en la certificación y validación de documentos académicos, especialmente en lo referente a la integridad y verificación confiable de la información. Este trabajo documenta el desarrollo de un prototipo de aplicación descentralizada para la gestión de certificaciones académica, utilizando la tecnología blockchain como solución innovadora que permite aprovechar sus propiedades para enfrentar estos retos. El estudio inicia con un análisis de la red blockchain y sus aplicaciones especialmente en el ámbito educativo, posteriormente se realiza una entrevista estructurada para comprender el proceso actual de generación de certificados académicos. Para el desarrollo de la aplicación, se adoptó la metodología de investigación aplicada, la cual proporciona un marco flexible adecuado para desarrollar un producto, se comienza con la propuesta del prototipo, en la que se recopilan las necesidades de los usuarios finales y se diseña el modelo de la aplicación, se describe la arquitectura del sistema y se emplean herramientas de código abierto y marcos de desarrollo que facilitan la integración de los distintos componentes del sistema con la red blockchain, una vez definido lo anterior se codifica y despliega el contrato inteligente donde se definen las reglas de negocio, finalmente se implementa una interfaz gráfica de usuario que permite la interacción directa con el contrato inteligente, brindando a los usuarios un acceso seguro y verificable a los certificados emitidos por el Instituto Académico de Idiomas.

Palabras clave: Blockchain, Smart contract, Certificación académica, Aplicaciones descentralizadas, Prototipo.

**Abstract.**

Higher education institutions face significant challenges in the certification and validation of academic documents, particularly concerning the integrity and reliable verification of information. This work presents the development of a decentralized application prototype for managing academic certifications, using blockchain technology as an innovative solution that leverages its properties to address these challenges. The study begins with an analysis of blockchain networks and their applications, particularly in the educational sector. A structured interview was conducted to understand the current process of generating academic certificates.  
To develop the application, an applied research methodology was adopted, providing a flexible framework suitable for creating a functional product. The process started with the design of the prototype, including the collection of end-user requirements and the modeling of the application. The system architecture is described, and open-source tools and development frameworks are used to facilitate the integration of the system components with the blockchain network. Once the previous steps were completed, the smart contract was coded and deployed, defining the business logic rules. Finally, a graphical user interface was implemented to allow users to interact directly with the smart contract, providing secure and verifiable access to the certificates issued by the Academic Language Institute.

# Índice general de contenidos

[Índice general de contenidos i](#_Toc198231607)

[Lista de tablas ii](#_Toc198231608)

[Lista de figuras ii](#_Toc198231609)

[Lista de anexos iii](#_Toc198231610)

[Capítulo 1 1](#_Toc198231611)

[1. Generalidades 1](#_Toc198231612)

[1.1. Introducción 1](#_Toc198231613)

[1.2. Antecedentes 1](#_Toc198231614)

[1.3. Planteamiento del problema 3](#_Toc198231615)

[1.4. Hipótesis y Justificación 4](#_Toc198231616)

[1.4.1. Hipótesis 4](#_Toc198231617)

[1.4.2. Justificación 4](#_Toc198231618)

[1.5. Objetivos 5](#_Toc198231619)

[1.5.1. General 5](#_Toc198231620)

[1.5.2. Específicos 5](#_Toc198231621)

[Capítulo 2 7](#_Toc198231622)

[2. Marco Teórico 7](#_Toc198231623)

[2.1. Conceptos 7](#_Toc198231624)

[2.1.1. Certificación 7](#_Toc198231625)

[2.1.2. Certificación Académica 7](#_Toc198231626)

[2.2. Blockchain 7](#_Toc198231627)

[2.2.1. Características de Blockchain 8](#_Toc198231628)

[2.2.2. Arquitectura de blockchain 9](#_Toc198231629)

[2.2.3. Bloque 9](#_Toc198231630)

[2.2.4. Mecanismo de Consenso 11](#_Toc198231631)

[2.3. Smart contracts 12](#_Toc198231632)

[2.3.1. Estructura de un smart contract 12](#_Toc198231633)

[2.4. Herramientas tecnológicas 13](#_Toc198231634)

[Capítulo 3 18](#_Toc198231635)

[3. Metodología experimental 18](#_Toc198231636)

[Capítulo 4 20](#_Toc198231637)

[4. Cálculos y resultados 20](#_Toc198231638)

[4.1. Propuesta del prototipo 20](#_Toc198231639)

[4.1.1. Propósito 20](#_Toc198231640)

[4.1.2. Alcance 20](#_Toc198231641)

[4.1.3. Identificación de procesos 21](#_Toc198231642)

[4.1.4. Identificar a los stakeholders 22](#_Toc198231643)

[4.1.5. Prototipo propuesto 22](#_Toc198231644)

[4.1.6. Funciones del prototipo 23](#_Toc198231645)

[4.1.7. Requisitos funcionales 30](#_Toc198231646)

[4.1.8. Requisitos No funcionales 31](#_Toc198231647)

[4.2. Descripción de la arquitectura 32](#_Toc198231648)

[4.3. Selección de herramientas 33](#_Toc198231649)

[4.4. Desarrollo del prototipo propuesto 35](#_Toc198231650)

[4.5. Interacción con el contrato inteligente 35](#_Toc198231651)

[Capítulo 5 36](#_Toc198231652)

[5. Conclusiones y recomendaciones 36](#_Toc198231653)

[5.1. Discusión de resultados 36](#_Toc198231654)

[5.2. Conclusiones 36](#_Toc198231655)

[5.3. Recomendaciones 36](#_Toc198231656)

[6. Referencias 37](#_Toc198231657)

[7. Anexos 42](#_Toc198231658)

# Lista de tablas

[Tab. 1. Ventajas e inconvenientes de una red blockchain. 13](#_Toc197013615)

[Tab. 2. Ventajas e inconvenientes del entorno de desarrollo integrado 15](#_Toc197013616)

[Tab. 3. Ventajas e inconvenientes de los diferentes lenguajes de programación 15](#_Toc197013617)

[Tab. 4. Hallazgos 21](#_Toc197013618)

[Tab. 5. Descripción de los actores 21](#_Toc197013619)

[Tab. 6. Autenticación y Autorización 25](#_Toc197013620)

[Tab. 7. Gestionar certificados 27](#_Toc197013621)

[Tab. 8. Validar Certificado 29](#_Toc197013622)

[Tab. 9. Requisitos funcionales 30](#_Toc197013623)

[Tab. 10. Requisitos no funcionales 30](#_Toc197013624)

# Lista de figuras

[Fig. 1. Estructura blockchain 8](#_Toc197013625)

[Fig. 2. Estructura de un bloque 9](#_Toc197013626)

[Fig. 3. Estructura de un contrato inteligente 12](#_Toc197013627)

[Fig. 4. Modelo propuesto: Certificación descentralizada de documentos académicos. 22](#_Toc197013628)

[Fig. 5. Funciones del prototipo de software, función nivel cero. 23](#_Toc197013629)

[Fig. 6. Diagrama de casos de uso para la autenticación y autorización, función en nivel uno. 24](#_Toc197013630)

[Fig. 7. Diagramas de caso para gestionar los certificados, función en nivel uno. 26](#_Toc197013631)

[Fig. 8. Diagramas de caso para validar los certificados, función en nivel uno. 28](#_Toc197013632)

[Fig. 9. Arquitectura propuesta de la aplicación. 32](#_Toc197013633)

# Lista de anexos

# Capítulo 1

## Generalidades

### Introducción

### 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 las 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

Los certificados académicos son documentos oficiales que respaldan el historial académico de una persona y que son emitido por el Instituto académico de Idiomas de la Universidad Central del Ecuador estos constituye un componente esencial en el perfil profesional de los estudiantes, sin embargo, los métodos actuales utilizados para emitir este tipo de certificados están sujetos a diversas situaciones que pueden generar inconvenientes, por ejemplo, la certificación y verificación de documentos académicos como títulos y certificados, sigue dependiendo en gran medida de procesos manuales y centralizados, esto conlleva a posibles problemas como la falsificación de documentos, perdida de información sensible, demoras en la verificación de la autenticidad y costos administrativos elevados, lo cual compromete la eficiencia, seguridad y confiabilidad del sistema de gestión documental académica.

Las soluciones basadas en el envío de documentos por correo electrónico, la transferencia de archivos en formato PDF y el uso de portales seguros para la entrega de certificados digitales son cada vez más comunes, aunque estas alternativas representan un avance hacia la digitalización aún presentan desafíos en términos de escalabilidad, integridad y verificación confiable [1].

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

Por ello, surge la necesidad de desarrollar un prototipo de aplicación basado en la tecnología 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 la emisión y verificación de certificados académicos, estos sistemas generalmente centralizados, incrementan la carga de trabajo administrativo especialmente a la hora de verificar la autenticidad de los documentos, los cuales pueden ser vulnerables a perdidas o falsificaciones, como resultado los estudiantes deben encargarse de conservar sus certificados para posteriormente integrarlos en su portafolio profesional.

Este proyecto propone el desarrollo de un prototipo para la certificación académica utilizando una blockchain, con el fin de aprovechar las ventajas que ofrece este tipo de tecnología, tales como, mantener los registros descentralizados, seguros, confiables y de acceso ágil, esto permitirá optimizar los procesos de validación de los certificados de culminación de un idioma emitidos por el Instituto Académico de Idiomas de la Universidad Central del Ecuador.

La adopción de esta tecnología en el ámbito educativo ofrece múltiples beneficios, como la eliminación de intermediarios en la validación de documentos reduciendo errores y tiempos de espera, también facilita el acceso inmediato a los registros académicos, eliminando la necesidad de solicitar documentos físicos. Además, de garantizar la autenticidad e inmutabilidad de la información reduciendo los riesgos de pérdidas o falsificación, y fortaleciendo la transparencia y confianza de los sistemas de gestión académica.

El impacto de esta propuesta no se limita a la Universidad Central del Ecuador, sino que también puede inspirar a otras instituciones de educación superior interesadas en modernizar sus procesos, transformando el sistema hacia entornos interconectados, abiertos y confiables, capaces de registrar con precisión el desempeño estudiantil 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 adecuada que permita mejorar la flexibilidad y eficiencia en el desarrollo del proyecto.

# 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 blockchain

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.

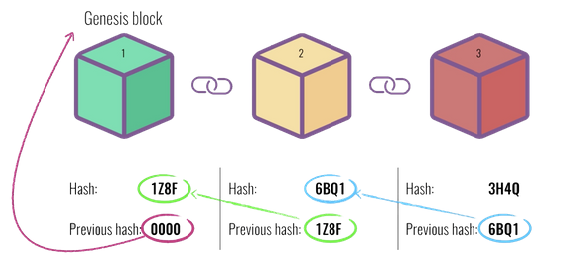


Fig. 1. Estructura blockchain

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. [14]

#### 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. [14]

#### 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. [15]

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 contract

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.

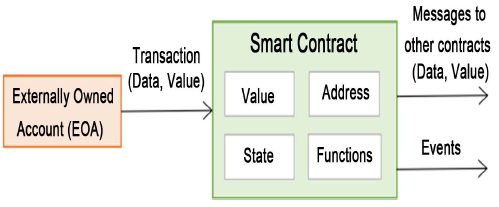


Fig. 3. Estructura de un contrato inteligente

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 [16]

### Herramientas tecnológicas

El desarrollo acelerado de la tecnología blockchain ha despertado un creciente interés en la implementación de redes descentralizadas que prioricen la seguridad y la transparencia, este avance ha dado origen a múltiples plataformas diseñadas para la creación y administración de redes blockchain, cada una con características, beneficios y retos particulares. La evolución constante de estas tecnologías responde, en gran parte, a la necesidad de soluciones innovadoras que afronten desafíos relacionados con la confianza, la protección de datos y la optimización de procesos en diversas industrias [17].

Para el desarrollo de la propuesta planteada en este trabajo, se analizaron distintas opciones de redes blockchain, entre las cuales destacan Ethereum (ETH), Hyperledger Fabric (FABRIC), Solana (SOL) y Polkadot (DOT). Cada una de estas plataformas presenta fortalezas y limitaciones que fueron consideradas en el análisis comparativo que se muestra en la Tabla 1.

|  |  |  |
| --- | --- | --- |
| **Red** | **Ventajas** | **Inconvenientes** |
| Ethereum (ETH) | Alta versatilidad para la ejecución de contratos inteligentes.  Plataforma de código abierto, accesible para cualquier desarrollador.  Amplia comunidad y ecosistema de desarrollo.  Seguridad robusta basada en mecanismos de consenso PoW. | Escalabilidad limitada y congestión en la red.  Privacidad estándar, menos adecuada para aplicaciones que requieren confidencialidad. |
| Hyperledger Fabric (FABRIC) | Orientación empresarial con funciones avanzadas.  Control de acceso detallado y privacidad granular.  Buena escalabilidad y eficiencia en entornos corporativos. | Configuración técnica más compleja.  Comunidad y soporte más reducidos en comparación con Ethereum. |
| Solana (SOL) | Alta velocidad de procesamiento (hasta 65,000 TPS).  Bajas tarifas de transacción y alto rendimiento.  Soporte completo para Turing, ideal para aplicaciones complejas. | Tecnología menos madura y con riesgo potencial.  Comunidad y ecosistema en desarrollo, pero aún limitados. |
| Polkadot (DOT) | Interoperabilidad entre múltiples blockchains.  Escalabilidad mejorada mediante el uso de cadenas paralelas. | Menor adopción y madures en comparación con Ethereum.  Mayor complejidad técnica para desarrolladores. |

Tab. 1. Ventajas e inconvenientes de una red blockchain.

Se eligió la red Ethereum debido a la amplia gama de herramientas que proporciona, su flexibilidad para la implementación de contratos inteligentes y el respaldo de una comunidad activa y consolidada. Su alto nivel de adopción y el desarrollo de un ecosistema sólido la posicionan como una de las plataformas más maduras del sector. Adicionalmente, Ethereum permite la creación de contratos inteligentes que operan con su criptomoneda nativa, lo cual facilita la implementación de incentivos económicos para los usuarios que interactúan con el sistema.

Para el desarrollo de la aplicación se consideraron tres entornos de desarrollo integrados (IDE): Remix, Truffle y Visual Studio (VS Code) cada uno de estos entornos ofrece características particulares orientadas al desarrollo, prueba y despliegue de contratos inteligentes [18]. La Tabla 2 detalla un análisis comparativo de sus principales ventajas y limitaciones desde una perspectiva técnica.

|  |  |  |
| --- | --- | --- |
| **IDE** | **Ventajas** | **Inconvenientes** |
| Remix | Plataforma accesible y fácil de usar, disponible de manera online.  Soporte completo para el desarrollo y despliegue de contratos inteligentes en Ethereum.  Amplia documentación y comunidad activa. | Funcionalidades limitadas en comparación con IDEs locales más avanzados.  Dependencia de una conexión a Internet para su uso. |
| Truffle | Potente suite de herramientas para el desarrollo de aplicaciones en Ethereum.  Permite el desarrollo local y pruebas integradas.  Proporciona herramientas avanzadas para testing, migración y despliegue de contratos. | Curva de aprendizaje empinada para desarrolladores novatos.  Requiere configuración local y dependencias adicionales. |
| VS Code | Integración con el popular editor de código Visual Studio Code.  Gran capacidad de personalización y soporte de una amplia comunidad. | Requiere configuración adicional y la instalación de extensiones.  Menor soporte nativo para Ethereum en comparación con Remix. |

Tab. 2. Ventajas e inconvenientes del entorno de desarrollo integrado

Se seleccionó Truffle debido a su interfaz amigable y su integración directa con la red Ethereum, lo que simplifica significativamente el proceso de desarrollo y depuración de contratos inteligentes. Adicionalmente, al estar basado en la web, permite la escritura, prueba y despliegue de contratos inteligentes en Ethereum de forma eficiente y accesible.

Existen varios lenguajes de programación empleados en el desarrollo de contratos inteligentes. En el marco de esta investigación, se han considerado como opciones principales Solidity y Vyper, cuyas ventajas y desventajas se detallan en la Tabla 3.

|  |  |  |
| --- | --- | --- |
| **Lenguaje** | **Ventajas** | **Inconvenientes** |
| Solidity | Diseñado específicamente para contratos inteligentes en la plataforma Ethereum.  Utiliza un enfoque orientado a objetos, permitiendo la creación de código reutilizable y fácil de mantener.  Amplia adopción y una comunidad activa que respalda su desarrollo.  Integración fluida con herramientas de desarrollo como Remix y Truffle. | Posibles vulnerabilidades y errores de seguridad debido a su complejidad.  Limitaciones al compararlo con lenguajes más maduros. |
| Vyper | Lenguaje más seguro y fácil de comprender en comparación con Solidity.  Diseño enfocado en la simplicidad y la seguridad.  Menos propenso a errores y vulnerabilidades de seguridad. | Menor adopción y una comunidad más reducida en comparación con Solidity.  Limitación en funcionalidades avanzadas, con menos soporte y herramientas de desarrollo disponibles. |

Tab. 3. Ventajas e inconvenientes de los diferentes lenguajes de programación

La opción de Vyper fue descartada debido a su menor adopción y a las restricciones que presenta frente a Solidity. Por otro lado, Solidity es ampliamente utilizado en el ecosistema Ethereum y se integra de forma nativa con herramientas como Remix. Está diseñado específicamente para la creación de contratos inteligentes, lo que lo convierte en la opción más adecuada para este caso de uso.

# 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 [19]. 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 [20].

Según Fidias [21], 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 [22], 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.

# Capítulo 4

## Cálculos y resultados

### Propuesta del prototipo

Antes de desarrollar el prototipo basado en tecnología blockchain, orientado a la emisión de certificados de culminación de estudios del idioma inglés en el Instituto Académico de Idiomas (IAI) de la Universidad Central del Ecuador, es fundamental identificar a los actores que intervienen directamente, ya que esto permitirá definir con claridad el modelo y diseño del producto propuesto. Una vez establecidos los stakeholders, se procederá a especificar los requerimientos funcionales de cada uno, definir la arquitectura del sistema, seleccionar la plataforma más adecuada para su implementación y, finalmente, se llevará a cabo el desarrollo del prototipo, seguido de pruebas para evaluar su funcionamiento y efectividad.

#### Propósito

Esta sección describe los aspectos clave relacionados con el diseño y desarrollo del prototipo, en función de la "Especificación de Requisitos de Software" (ERS). La aplicación web resultante servirá como una herramienta para gestionar la verificación y validación de la autenticidad de los certificados de suficiencia emitidos por el Instituto Académico de Idiomas, haciendo uso de la tecnología blockchain y contratos inteligentes. Además, la documentación generada ofrece a todos los actores involucrados una visión detallada de la perspectiva del proyecto y una comprensión general del prototipo de software.

#### Alcance

La aplicación web que se desarrollará actuará como un prototipo de demostración de una plataforma descentralizada para la certificación de documentos académicos, la misma que permitirá gestionar el perfil del administrador autorizado encargado de emitir los certificados a los usuarios finales. El Instituto Académico de Idiomas tendrá la capacidad de generar los certificados para su validación y certificación, mientras que los usuarios finales, ya sean estudiantes o instituciones externas podrán acceder a la información y obtener el certificado digital. El propósito principal de este prototipo es eliminar la intermediación de terceros en los procesos de certificación académica del idioma inglés, estableciendo un canal directo entre la institución y los estudiantes. De esta manera, se garantiza la disponibilidad y autenticidad de la información, reforzando la confianza en el sistema de certificación académica.

#### Identificación de procesos

Para comprender el alcance de la aplicación e identificar a los actores clave dentro del sistema, se llevaron a cabo entrevistas en el Instituto Académico de Idiomas de la Universidad Central del Ecuador. Este proceso permitió analizar los principales desafíos asociados a la verificación y certificación académica. En la tabla 4 se presentan los hallazgos obtenidos a partir de estas entrevistas, los cuales sirvieron de base para definir los requisitos funcionales del sistema.

|  |  |
| --- | --- |
| **Dominio de la información** | **Hallazgo** |
| Almacenamiento de la información de los estudiantes | La información de los estudiantes se almacena en la PC del instituto académico. En esta se almacena el historial de solicitudes atendidas y no atendidas. |
| Áreas encargadas de la emisión de certificados académicos. | Inicialmente, el área de TI se encarga de gestionar y administrar la información mediante la plataforma SIIU. Por otro lado, el área de Secretaría genera el certificado, y posteriormente, el área de Dirección valida y autentica el documento. Finalmente, el certificado es enviado al estudiante. |
| Áreas encargadas de la verificación los certificados académicos | En primer lugar, se encuentra el área de admisiones, encargada de hacer el seguimiento de los registros académicos de los estudiantes. Por otro lado, una entidad externa recibe la información necesaria para proceder con la validación notarial del certificado. |
| Problema identificado | Actualmente, en el IAI no existe ningún mecanismo ágil ni seguro para verificar la autenticidad de los certificados digitales. |

Tab. 4. Hallazgos

#### Identificar a los stakeholders

Para identificar a los stakeholders, es fundamental analizar qué actores van a interactuar con el prototipo de la aplicación, esto permitirá determinar el rol de cada participante dentro del sistema y la relación entre ellos. Basándonos en la sección anterior de este documento, se pueden identificar los siguientes actores que se muestra en la tabla 5:

|  |  |
| --- | --- |
| **Rol** | **Descripción** |
| Estudiante | Él es el actor que recibe el certificado emitido por el Instituto Académico de Idiomas. |
| Instituto Académico de Idiomas (Administrador) | Es el actor encargado de emitir y validar los certificados. Tiene la capacidad de generar, almacenar y enviar los certificados tanto al estudiante como a otras dependencias de la universidad. |
| Otras dependencias de la Universidad | Este actor tiene la capacidad de consultar los certificados del estudiante, los cuales han sido previamente validados por el Instituto Académico de Idiomas. |

Tab. 5. Descripción de los actores

#### Prototipo propuesto

La gestión de certificados académicos en el Instituto Académico de Idiomas involucra procedimientos administrativos complejos, que frecuentemente requieren la participación de otras dependencias dentro de la Universidad. A través de la adopción de tecnologías emergentes como blockchain y los contratos inteligentes, es posible implementar un modelo descentralizado que proporcione mecanismos de confianza e integridad entre las áreas involucradas en la administración de certificados académicos, como se ilustra en la figura 4. Bajo este enfoque, se propone desarrollar una solución tecnológica que permita la generación digital de certificados académicos para los estudiantes, cuyo registro se realice como una transacción inmutable en una red blockchain.

En este contexto, los usuarios finales podrán interactuar con la plataforma mediante contratos inteligentes, lo que les permitirá obtener, validar y consultar sus certificados de forma autónoma y segura. Este mecanismo garantiza la validación y verificación inmediata de los documentos, permitiendo a los interesados consultar y comprobar su autenticidad con rapidez y fiabilidad.

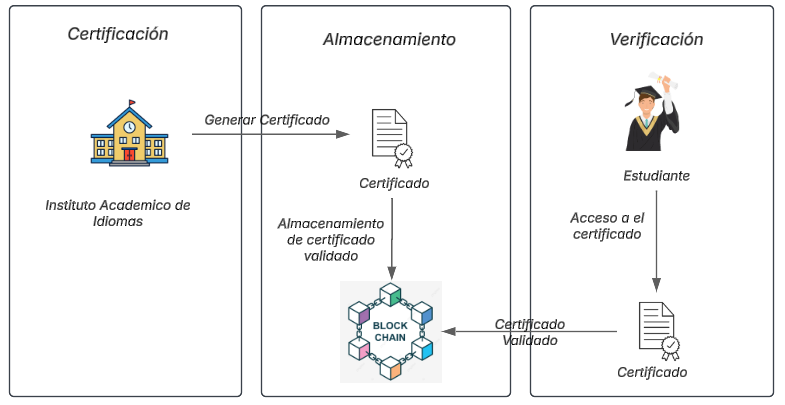


Fig. 4. Modelo propuesto: Certificación descentralizada de documentos académicos.

#### Funciones del prototipo

Este segmento describe las funciones específicas del sistema orientadas en la emisión y validación de certificados académicos, considerando el perfil del usuario que interactúa con él. El enfoque principal es analizar las operaciones que debe realizar el sistema, resaltando la autentificación de los certificados de culminación de un idioma como un caso de uso esencial. El primer caso de uso de nivel cero se presenta en la Figura 5, en la cual se detallan las principales funcionalidades del actor responsable de validar el certificado y del usuario final, en el proceso de generación segura de los certificados académicos.

Diagrama

El contenido generado por IA puede ser incorrecto.

Fig. 5. Funciones del prototipo de software, función nivel cero.

Como se puede visualizar, el prototipo de software está conformado por tres funciones principales.

En la primera funcionalidad consideramos la autentificación y autorización para poder acceder a la plataforma, esta funcionalidad permite asegurar el ingreso restringido de usuarios autorizados.

Segundo gestionar certificado, es donde el administrador autorizado genera el certificado en la blockchain.

Tercero, permite a los usuarios finales verificar la autenticidad del certificado digital, asegurando la disponibilidad y la inmutabilidad de estos.

Estas funcionalidades se presentan en su forma más elemental. Cada caso de uso ilustra cómo el sistema interactúa con los distintos actores, proporcionando un escenario representativo. Con el fin de facilitar una mejor comprensión, dichos casos serán desarrollados en un nivel de mayor detalle, denominado nivel uno. Para ello, se dividirán en funciones más específicas. El primer caso de uso se encuentra representado en la Figura 6.

Diagrama

El contenido generado por IA puede ser incorrecto.

Fig. 6. Diagrama de casos de uso para la autenticación y autorización, función en nivel uno.

El ingreso al sistema por parte del usuario administrador se realiza mediante un mecanismo de autenticación, el cual actúa como punto de control para restringir el acceso a las funcionalidades del sistema. Tras la validación de credenciales, el sistema identifica el perfil del usuario y habilita el acceso a las secciones correspondientes. En el caso del perfil de administrador, se le otorgan permisos completos para gestionar los certificados, mientras que los usuarios con perfil del estudiante acceden únicamente a las funcionalidades relacionadas con la verificación de certificados previamente validados.

|  |  |  |  |
| --- | --- | --- | --- |
| **CU – 01** | **Autenticación y Autorización** | | |
| **Versión** | 1.0 | | |
| **Precondición** | El usuario con perfil de administrador debe acceder a la plataforma para iniciar sesión o completar el proceso de registro. | | |
| **Descripción** | Este caso de uso describe el comportamiento del sistema durante el proceso de autenticación y autorización, permitiendo el acceso controlado. | | |
| **Secuencia normal** | **Caso de uso (Nivel Uno)** | **Acción** | |
| **1** | Iniciar sesión: El usuario inicia el proceso de autenticación ingresando sus credenciales en el formulario correspondiente. | |
| **2** | Registrarse: Si el usuario no posee una cuenta, puede acceder a la opción de registro para crear un perfil dentro de la plataforma. | |
| **3** | Llenar Formulario: El sistema solicita al usuario completar un formulario con los datos requeridos para crear su perfil. | |
| **4** | Recuperar clave: Si el usuario olvido o necesita actualizar su clave, el sistema ofrece un mecanismo para restablecer la contraseña. | |
| **Postcondición** | Una vez autenticado, el usuario podrá gestionar los certificados de los estudiantes. | | |
| **Excepciones:** | **Referencia al caso de uso** | **Acción** | |
| **3** | Si el usuario no completa todos los campos obligatorios del formulario de registro. | |
| **E1** | El sistema muestra un mensaje indicando que todos los campos requeridos deben completarse. |
| **Comentarios** | El administrador podrá crear un perfil desde el cual gestionará la emisión y validación de certificados digitales dentro de la plataforma. | | |

Tab. 6. Autenticación y Autorización

En la figura 7 se presenta el diagrama de caso de uso correspondiente a la funcionalidad de gestión de certificados, asignada al administrador autorizado por el Instituto Académico de Idiomas. Para acceder a estas operaciones, el administrador debe autenticarse previamente en la plataforma. Esta funcionalidad contempla las acciones de generación, almacenamiento, búsqueda y visualización de certificados de culminación de un idioma.

Diagrama

El contenido generado por IA puede ser incorrecto.

Fig. 7. Diagramas de caso para gestionar los certificados, función en nivel uno.

La Tabla 7 describe la funcionalidad del sistema relacionada con la gestión de certificados académicos digitales. En este contexto, el administrador autorizado posee la facultad y la responsabilidad de generar nuevos certificados y consultar el certificado de un estudiante en específico garantizando la integridad, disponibilidad y autenticidad de estos documentos.

|  |  |  |  |
| --- | --- | --- | --- |
| **CU – 02** | **Gestionar Certificado** | | |
| **Versión** | 1.0 | | |
| **Dependencias** | CU-01 | | |
| **Precondición** | El administrador debe estar autenticado en la plataforma. | | |
| **Descripción** | Este caso de uso describe la funcionalidad de la plataforma que permite al administrador generar, almacenar, buscar y visualizar certificados académicos. | | |
| **Secuencia normal** | **Caso de uso (Nivel Uno)** | **Acción** | |
| **1** | **Generar certificado:** El administrador ingresa los datos del estudiante para generar el certificado académico correspondiente. | |
| **2** | **Almacenar certificado:** El sistema almacena el hash del certificado en la blockchain y los datos relevantes en la base de datos del sistema. | |
| **3** | **Buscar certificado:** La plataforma permite al administrador realizar búsquedas de certificados almacenados en la red blockchain. | |
| **4** | **Visualizar certificado:** El administrador puede visualizar todos los certificados generados dentro de la plataforma. | |
| **Postcondición** | El administrador carga los certificados y genera su certificación en la blockchain, asegurando su integridad y disponibilidad. | | |
| **Excepciones:** | **Referencia al caso de uso** | **Acción** | |
| **3** | Si el administrador intenta generar un certificado duplicado. | |
| **E1** | El sistema informa que el certificado no ha sido emitido y evita la duplicación. |
| **Comentarios** | Este caso de uso permite al administrador gestionar totalmente los certificados garantizando la integridad, disponibilidad y autenticidad de la información. | | |

Tab. 7. Gestionar certificados

En la Figura 8 se presenta el diagrama de caso de uso asociado al usuario final, correspondiente a la función de validación de certificados emitidos por el Instituto Académico de Idiomas. Esta funcionalidad permite al usuario acceder a la plataforma, consultar su certificado, visualizarlo, descargarlo y compartirlo. Las acciones vinculadas a esta operación, según el perfil del usuario final, se representan en dicho esquema.

Diagrama

El contenido generado por IA puede ser incorrecto.

Fig. 8. Diagramas de caso para validar los certificados, función en nivel uno.

La Tabla 8 describe el caso de uso asociado a la validación de certificados digitales por parte del usuario final, quien, mediante la introducción de su número de cédula, puede verificar la autenticidad de su certificado, visualizarlo, descargarlo en formato PDF o compartirlo a través de un enlace. Este proceso se realiza de manera eficiente y segura, garantizando la disponibilidad, integridad y autenticidad del certificado dentro de la plataforma.

|  |  |  |  |
| --- | --- | --- | --- |
| **CU – 03** | **Validar Certificado** | | |
| **Versión** | 1.0 | | |
| **Precondición** | El usuario final debe tener su número de cedula. | | |
| **Descripción** | Este caso de uso describe la funcionalidad destinada al usuario final para validar certificados académicos emitidos por el Instituto Académico de Idiomas. La operación contempla la consulta, visualización, descarga y opción de compartir el certificado digital. | | |
| **Secuencia normal** | **Caso de uso (Nivel Uno)** | **Acción** | |
| **1** | **Consultar certificado:** El usuario accede a la plataforma e introduce los datos requeridos para localizar su certificado. | |
| **2** | **Descargar certificado:** El usuario puede descargar el documento digital certificado desde la plataforma en formato PDF. | |
| **3** | **Compartir certificado:** La plataforma ofrece opciones para compartir el certificado a través de medios digitales. | |
| **Postcondición** | El usuario accede exitosamente a su certificado, pudiendo visualizarlo, descargarlo o compartirlo, validando su autenticidad. | | |
| **Excepciones:** | **Referencia al caso de uso** | **Acción** | |
| **3** | Si el usuario ingresa datos incorrectos o el certificado no está disponible en el sistema. | |
| **E1** | El sistema informa al usuario que no se ha encontrado un certificado asociado a los datos ingresados. |
| **Comentarios** | Este caso de uso permite al usuario final verificar directamente sus documentos emitidos por el Instituto Académico de Idiomas, asegurando su disponibilidad y autenticidad. | | |

Tab. 8. Validar Certificado

#### Requisitos funcionales

Los requisitos funcionales definen las acciones específicas que el sistema debe ejecutar para cumplir con los objetivos del proyecto. A partir del análisis de los casos de uso, estos requisitos han sido identificados, clasificados e indexados mediante etiquetas que facilitan su referencia y comprensión. La Tabla 9 resume las funcionalidades clave previstas para la plataforma, estableciendo la relación directa con los casos de uso correspondientes.

|  |  |  |
| --- | --- | --- |
| Requerimiento | Descripción | Caso de uso |
| RF-1 | El sistema debe permitir que un usuario autorizado inicie sesión en la plataforma, siempre que se encuentre previamente registrado. | CU-01-1 |
| RF-2 | El sistema debe ofrecer al administrador la opción de registrarse en la plataforma. | CU-01-2 |
| RF-3 | El sistema debe presentar al usuario un formulario de registro con los campos requeridos para crear su perfil. | CU-01-3 |
| RF-4 | El sistema debe permitir al administrador recuperar y restablecer su contraseña en caso de olvido o actualización. | CU-01-4 |
| RF-5 | El sistema debe permitir al administrador ingresar los datos necesarios del estudiante para la generación del certificado. | CU-01-5 |
| RF-6 | El sistema debe almacenar el hash del certificado generado en la blockchain y los datos en la base de datos. | CU-02-1 |
| RF-7 | El sistema debe permitir al administrador buscar certificados académicos dentro de la plataforma. | CU-02-2 |
| RF-8 | El sistema debe permitir al administrador visualizar el listado de certificados generados. | CU-02-3 |
| RF-9 | El sistema debe permitir al usuario final consultar la existencia y validez de su certificado digital. | CU-02-4 |
| RF-10 | El sistema debe permitir al usuario final visualizar el contenido de su certificado digital. | CU-03-1 |
| RF-11 | El sistema debe permitir al usuario final descargar su certificado en formato PDF. | CU-03-2 |
| RF-12 | El sistema debe permitir al usuario final compartir un enlace de acceso a su certificado validado. | CU-03-3 |

Tab. 9. Requisitos funcionales

#### Requisitos No funcionales

|  |  |
| --- | --- |
| Requisito | Descripción |
| RNF-1 | Para fines de desarrollo y pruebas, la plataforma será implementada y desplegada en un entorno local controlado. |
| RNF-2 | La interfaz de usuario debe ofrecer una experiencia intuitiva, clara y fácil de usar, priorizando la simplicidad en la navegación. |
| RNF-3 | La plataforma debe estar optimizada para minimizar los tiempos de procesamiento y la carga del servidor al momento de visualizar un certificado. |
| RNF-4 | El sistema debe proporcionar una experiencia fluida y sin latencias significativas durante la descarga de certificados digitales. |
| RNF-5 | La arquitectura del sistema debe permitir un mantenimiento sencillo y actualizaciones periódicas, garantizando la continuidad operativa y la corrección eficiente de errores. |
| RNF-6 | Toda información sensible, incluyendo datos personales y certificados, debe ser almacenada y transmitida mediante mecanismos de cifrados seguros (como HTTPS y algoritmos de encriptación estándar). |

Tab. 10. Requisitos no funcionales

El cumplimiento de los requisitos no funcionales de la tabla 10 es fundamental para garantizar la eficiencia operativa, la seguridad de los datos y la escalabilidad del sistema. Estos criterios complementan los requisitos funcionales al asegurar que la plataforma no solo cumpla con sus objetivos técnicos, sino que también lo haga de manera segura, confiable y con una experiencia de usuario optimizada.

### Descripción de la arquitectura

Para el desarrollo de una aplicación descentralizada (DApp) orientada al ámbito educativo, se han considerado elementos clave como la tecnología blockchain, los contratos inteligentes, la descentralización y la certificación digital. La solución propuesta se estructura en una arquitectura de múltiples capas, lo que permite una integración eficiente de estas tecnologías.

Capa de presentación: Esta capa constituye la interfaz gráfica del sistema, permitiendo la interacción del usuario con la DApp. Se emplean tecnologías como React.js para la construcción de interfaces dinámicas, Bootstrap para el diseño responsivo y Web3.js para facilitar la comunicación directa con la red blockchain de Ethereum, está permite la lectura y escritura de datos en la blockchain, asegurando una interacción segura y transparente con los contratos inteligentes.

Capa lógica o de negocio: En esta capa se gestiona la lógica principal de la aplicación y su comunicación con la base de datos, por lo tanto, se implementa Node.js junto con el framework Express.js permitiendo un desarrollo robusto del backend. La persistencia de datos se maneja mediante MongoDB, una base de datos NoSQL utilizada para guardar información relevante de los usuarios y sus certificaciones académicas.

Capa blockchain: Esta capa es responsable de la gestión descentralizada de las operaciones críticas de la aplicación. Se implementan contratos inteligentes utilizando el lenguaje Solidity, desplegados sobre la red Ethereum, que garantizan la inmutabilidad, trazabilidad y seguridad en la emisión y validación de certificados. Para fines de desarrollo y pruebas, se hace uso de Ganache, una blockchain local que permite la simulación de un entorno Ethereum controlado, lo cual facilita la depuración y validación de los contratos. Además, se contempla el uso de Fruffle como herramienta para la migración y compilación de los contratos inteligentes.

Interfaz de usuario gráfica, Aplicación

El contenido generado por IA puede ser incorrecto.

Fig. 9. Arquitectura propuesta de la aplicación.

### Selección de herramientas

A partir del prototipo propuesto, así como de la arquitectura de aplicación y las plataformas expuestas en los capítulos anteriores, se ha elegido un conjunto específico de herramientas para el desarrollo de la plataforma descentralizada orientada al sector educativo. A continuación, se describirán detalladamente las herramientas seleccionadas.

**React.js:** Es una biblioteca de JavaScript de código abierto que ofrece una gran flexibilidad en el desarrollo de interfaces de usuario. Su arquitectura se basa en el uso de componentes reutilizables, cada uno con una función específica, lo que permite construir aplicaciones de forma modular y escalable. Estos componentes pueden gestionar sus propios estados, facilitando la creación de interfaces más organizadas, dinámicas y fáciles de mantener. [23]

**Express JS:** Es uno de los frameworks back-end más utilizados en el entorno de desarrollo con Node.js, diseñado con el propósito de facilitar la construcción de aplicaciones web. Se destaca por su simplicidad y flexibilidad, al ofrecer una amplia variedad de herramientas preconfiguradas que optimizan el rendimiento y agilizan el proceso de desarrollo [24].

**MongoDB:** Sistema de gestión de bases de datos NoSQL que almacena la información en colecciones de documentos, utilizando específicamente el formato BSON (Binary JSON). Gracias a su arquitectura altamente flexible, MongoDB se posiciona como una solución robusta para la gestión de datos, ofreciendo capacidades avanzadas de escalabilidad, consistencia, tolerancia a fallos, agilidad y flexibilidad. Estas características lo convierten en una herramienta ideal para entornos que requieren un desarrollo ágil y operaciones con mínima interrupción del servicio [24].

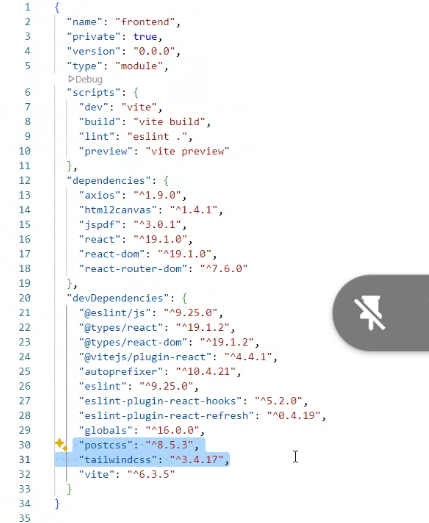
**Bootstrap:** Entorno gratuito y de código abierto ampliamente utilizado en el desarrollo web. Su propósito principal es facilitar la creación de sitios web responsivos y adaptables a dispositivos móviles, mediante el uso de clases CSS predefinidas. Además, puede instalarse fácilmente a través de NPM y ofrece compatibilidad con las versiones más recientes de los navegadores más utilizados [23].

**Web3.js:** Es una biblioteca desarrollada en el lenguaje Java, diseñada para ser ligera y reactiva. Su principal objetivo es facilitar la interacción con la blockchain de Ethereum mediante protocolos de comunicación como HTTP, IPC o Web Sockets. Esta herramienta permite integrarse fácilmente con un nodo de la red, lo que simplifica el desarrollo de aplicaciones descentralizadas (DApps). Además, Web3j ofrece funcionalidades para la creación y gestión de cuentas, así como para el despliegue y la carga de contratos inteligentes en una red de Ethereum previamente configurada [25].

**Metamask:** Extensión para navegadores web diseñada para facilitar la interacción entre las aplicaciones descentralizadas (DApps) y el entorno del navegador. Su propósito principal es actuar como un intermediario entre el usuario y la red blockchain, permitiendo la gestión segura de cuentas y la visualización de los criptoactivos asociados a una entidad [26].

**Truffle:** Se trata de uno de los frameworks más populares para el desarrollo sobre la plataforma Ethereum. Entre sus principales funcionalidades se encuentran la compilación, enlace y despliegue de contratos inteligentes directamente desde el entorno del framework. Además, permite realizar pruebas automatizadas y tareas de depuración para validar el correcto funcionamiento de los contratos. Este entorno también incluye herramientas para la gestión de scripts de despliegue y migración, tanto en redes públicas como privadas. [27]

### Desarrollo del prototipo propuesto



### Interacción con el contrato inteligente

# Capítulo 5

## Conclusiones y recomendaciones

### Discusión de resultados

Buscar de tesis similares y resumir de al menos 8

### Conclusiones

### Recomendaciones

## Referencias

|  |  |
| --- | --- |
| [1] | M. P. Jaramillo y N. Piedra, «IEEE Xplore,» Use of blockchain technology for Academic Certification in Higher Education Institutions, 19 03 2021. [En línea]. Available: https://ieeexplore.ieee.org/abstract/document/9381181. [Último acceso: 13 9 2024]. |
| [2] | A. Badr, L. Rafferty, Q. H. Mahmoud y K. Elgazzar, «IEEE Xplore,» A Permissioned Blockchain-Based System for Verification of Academic Records, 24 06 2019. [En línea]. Available: https://ieeexplore.ieee.org/document/8763831. [Último acceso: 13 9 2024]. |
| [3] | I. Alnafrah, «ScienceDirect,» Revitalizing blockchain technology potentials for smooth academic records management and verification in low-income countries, 9 09 2021. [En línea]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0738059321001139?via%3Dihub. [Último acceso: 14 9 2024]. |
| [4] | M. Morales Morales, L. Rosero Correa y S. Morales Cardoso, «REPOSITORIO INSTITUCIONAL UNIVERSIDAD CENTRAL DEL ECUADOR,» Registro de títulos académicos mediante una aplicación basada en Blockchain y Smart Contracts, 29 05 2020. [En línea]. Available: https://revistadigital.uce.edu.ec/index.php/CATEDRA/article/view/2200. [Último acceso: 14 9 2024]. |
| [5] | V. Gómez Bocanegra, G. S. García-delaTorre, C. A. PantojaMeléndeza y B. Loose Rojo, «ScienceDirect,» Blockchain aplicado en afecciones mamarias: desafíos y consideraciones éticas, 05 11 2024. [En línea]. Available: https://www.sciencedirect.com/science/article/pii/S021415822400080X. [Último acceso: 21 9 2024]. |
| [6] | R. I. Lara Moran, «Repositorio Institucional de la Universidad Politécnica Salesiana,» Arquitectura de información para asegurar la trazabilidad en la distribución de medicina en el Ministerio de Salud Pública basado en Blockchain, 23 07 2024. [En línea]. Available: http://dspace.ups.edu.ec/handle/123456789/29313. [Último acceso: 21 9 2024]. |
| [7] | F. J. Miranda González., A. Chamorro Mera y S. Rubio Lacoba, «Revistas ICE,» Clarificando el concepto de certificación: El caso español, 28 11 2004. [En línea]. Available: https://www.revistasice.com/index.php/BICE/article/view/3690. [Último acceso: 8 10 2024]. |
| [8] | C. Reyes Sáncheza, «Interconectando Saberes,» Blockchain: Funcionamiento y pertinencia en sectores públicos y privados, 17 08 2022. [En línea]. Available: https://is.uv.mx/index.php/IS/article/view/2734. [Último acceso: 8 10 2024]. |
| [9] | C. Kuchkovsky, G. Gómez Lardies, D. Díez García y Í. Molero, «Google academico,» BLOCKCHAIN: LA REVOLUCIÓN INDUSTRIAL DE INTERNET, 2017. [En línea]. Available: https://www.planetadelibros.cl/libros\_contenido\_extra/36/35615\_Blockchain.pdf. [Último acceso: 8 10 2024]. |
| [10] | C. Zozaya, J. Incera y L. A. Franzoni, «Google Academico,» BLOCKCHAIN: UN TUTORIAL, 2019. [En línea]. Available: https://scholar.google.es/scholar?hl=es&as\_sdt=0%2C5&q=BLOCKCHAIN%3A+UN+TUTORIAL&btnG=. [Último acceso: 8 10 2024]. |
| [11] | B. Murthy, Lawanya Shri, K. Seifedine y S. Lim, «IEEE Xplore,» Blockchain Based Cloud Computing: Architecture and Research Challenges, 11 09 2020. [En línea]. Available: https://ieeexplore.ieee.org/abstract/document/9252909. [Último acceso: 8 10 2024]. |
| [12] | J. G. Orosco Pantoja y J. J. Sánchez Lucas, «REPOSITORIO INSTITUCIONAL UNIVERSIDAD CENTRAL DEL ECUADOR,» Desarrollo de un prototipo de aplicación para la gestión de derechos de autor de obras musicales basado en tecnología blockchain y smart contract, 2023. [En línea]. Available: https://www.dspace.uce.edu.ec/entities/publication/463ef5e6-5ed3-4976-b8a3-0453372b9ca1. [Último acceso: 8 10 2024]. |
| [13] | Á. Santos García, «REPOSITORIO UNIVERSIDAD CARLOS III DE MADRID,» Caracterización de Smart Contracts en Ethereum, 18 10 2019. [En línea]. Available: https://e-archivo.uc3m.es/entities/publication/080c2dc1-e2b3-46a5-aa60-6478bbf607ab. [Último acceso: 31 10 2024]. |
| [14] | Z. Zibin, X. Shaoan , D. Hongning , C. Xiangping y W. Huaimin , «IEEE Xplore,» 25 9 2017. [En línea]. Available: https://ieeexplore.ieee.org/document/8029379. |
| [15] | Satoshi Nakamoto, «bitcoin.org,» Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer, 2008. [En línea]. Available: https://bitcoin.org/files/bitcoin-paper/bitcoin\_es.pdf. [Último acceso: 31 10 2024]. |
| [16] | K. M. Bhabendu, P. Soumyashree y J. Debasish , «IEEE Xplore,» An Overview of Smart Contract and Use Cases in Blockchain Technology, 18 10 2018. [En línea]. Available: https://ieeexplore.ieee.org/abstract/document/8494045. [Último acceso: 15 11 2024]. |
| [17] | B. F. Ocaña Valdez, «Repositorio Institucional de la Universidad Politécnica Salesiana,» Desarrollo de un prototipo de una criptomoneda con herramientas de código abierto basado en Ethereum de la Universidad Politécnica Salesiana, 02 2024. [En línea]. Available: https://dspace.ups.edu.ec/handle/123456789/26831. [Último acceso: 15 11 2024]. |
| [18] | . D. F. Hernández Formento, «Repositorio Universidad de Sevilla,» Análisis y capacidades de la tecnología Blockchain en el ámbito de la acreditación Académica., 26 06 2024. [En línea]. Available: https://idus.us.es/items/25eaf1c7-dc3e-4926-9e5c-33758fcc3ea3. [Último acceso: 15 11 2024]. |
| [19] | J. Ramirez, B. Castillo, J. C. Benavides y Y. Peralta, «E Nicaragua - Revista de La Universidad Autónoma,» Metodología de la Investigación e Investigación Aplicada para Ciencias Económicas y Administrativas, 2018. [En línea]. Available: https://jalfaroman.wordpress.com/wp-content/uploads/2019/03/dosier-metodologia-e-investigacion-aplicada-2018.pdf. [Último acceso: 5 3 2025]. |
| [20] | M. A. Lopera Vélez, «Google Scholar,» METODOLOGÍA DE LA INVESTIGACIÓN, 2012. [En línea]. Available: https://d1wqtxts1xzle7.cloudfront.net/31872466/2.\_METODOLOGIA\_DE\_LA\_INVESTIGACION-libre.pdf?1392460870=&response-content-disposition=inline%3B+filename%3DMETODOLOGIA\_DE\_LA\_INVESTIGACION\_Metodolo.pdf&Expires=1740691871&Signature=ZzuqUQ6ELNci3gCZL0FSfnDOS~s. [Último acceso: 5 03 2025]. |
| [21] | F. Arias, «Introducción a la metodología científica,» de *El proyecto de investigación*, 6ta ed., Caracas-República Bolivariana de Venezuela, Episteme, 2006, p. 143. |
| [22] | J. Lozada, «Dialnet,» Investigación Aplicada: Definición, Propiedad Intelectual e Industria, 12 2014. [En línea]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=6163749. [Último acceso: 5 3 2015]. |
| [23] | J. Marugán Rivilla, «REPOSITORIO UNIVERSIDAD POLITÉCNICA DE MADRID,» 07 2019. [En línea]. Available: https://oa.upm.es/62849/. |

# 

## Anexos