

**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.**

**Prototipo de aplicación para la creación y acceso a un aval de culminación de estudios superiores basado en la tecnología blockchain.**

Trabajo de titulación, modalidad proyecto de investigación presentado como requisito para aprobar el trabajo de titulación, para optar el título de Ingeniero en Informática.

**FELICITA VASCO HENRY PAOLO**

**TUTOR:** **Ing. Santiago Morales Cardoso. PhD**

Quito, 2024

Contenido

[INTRODUCCIÓN 3](#_Toc179445865)

[ANÁLISIS DEL PROBLEMA 3](#_Toc179445866)

[ANTECEDENTES 3](#_Toc179445867)

[PLANTEAMIENTO DEL PROBLEMA 4](#_Toc179445868)

[HIPÓTESIS Y JUSTIFICACIÓN 4](#_Toc179445869)

[HIPÓTESIS 4](#_Toc179445870)

[JUSTIFICACIÓN 4](#_Toc179445871)

[OBJETIVOS 5](#_Toc179445872)

[OBJETIVO GENERAL 5](#_Toc179445873)

[OBJETIVOS ESPECÍFICOS 5](#_Toc179445874)

[MARCO TEÓRICO 5](#_Toc179445875)

[Metodología experimental 5](#_Toc179445876)

[Cálculos y resultados 5](#_Toc179445877)

[Discusión de resultados 5](#_Toc179445878)

[Conclusiones 5](#_Toc179445879)

[Recomendaciones 5](#_Toc179445880)

[Bibliografía 5](#_Toc179445881)

[Anexos 6](#_Toc179445882)

# INTRODUCCIÓN

# ANÁLISIS DEL PROBLEMA

## ANTECEDENTES

Las instituciones educativas almacenan grandes volúmenes de expedientes, certificados y títulos académicos, a menudo los estudiantes solicitan dicha información para la transferencia de créditos, becas estudiantiles, seguros, cambio de carrera o requisitos previos para la aceptación en nuevos programas académicos. Si bien la transferencia de expedientes académicos es una actividad diaria habitual para las instituciones, a menudo conlleva importantes gastos, ya que el proceso de transferencia y verificación es extremadamente manual. (Badr, Rafferty, Mahmoud, & Elgazzar, 2019)

Además del acceso difícil y a veces imposible a los registros académicos de los estudiantes, y graduados en lo que respecta a la emisión, verificación y acreditación de certificados es largo y costoso tanto para ellos como para las universidades.

La necesidad de una solución automatizada de extremo a extremo para la transferencia y verificación de registros académicos está al límite, así como para proporcionar un método de verificación confiable que evite el fraude académico. (Badr, Rafferty, Mahmoud, & Elgazzar, 2019)

Los problemas asociados con la emisión de certificados académicos existen en todos los países y amenazan la integridad de las instituciones educativas, incluso en las más prestigiosas, como el Instituto Tecnológico de Massachusetts. (Alnafrah, 2021)

En ese sentido las cadenas de bloques podrían abordar tales retos a través del despliegue de una plataforma abierta, descentralizada, y directa, en donde se pueda desintermediar el flujo de información, logrando que se pueda mejorar la transparencia y la confianza en los registros educativos.

La tecnología Blockchain (BC) promete grandes beneficios tecnológicos en diferentes áreas como la agricultura, salud, educación, el gobierno entre otros. En el ámbito educativo, esta tecnología permite eliminar cuellos de botella en algunos procesos, además, brinda mayor seguridad en las transacciones realizadas y protección de la información de las instituciones. (Jaramillo & Piedra, 2020)

BC es una tecnología emergente introducida en 2008. Se utilizó por primera vez como un libro de contabilidad peer-to-peer para registrar las transacciones de la criptomoneda Bitcoin. El objetivo era eliminar cualquier intermediario tercero y permitir a los usuarios realizar sus transacciones directamente. (Alammary, Alhazmi, Almasri, & Gillani, 2019)

## PLANTEAMIENTO DEL PROBLEMA

La mayoría de las instituciones educativas continúan dependiendo de algunos procedimientos convencionales para la emisión y certificación de títulos académicos. Estos procesos pueden demorar unos días hasta más de un mes. Además de posibles daños físicos o perdidas de los registros durante todo el proceso. Las soluciones basadas en correo electrónico, transferencia de registros PDF y portales de entregas seguros, para la verificación de títulos o certificados en línea son cada vez más comunes. Si bien estas soluciones tienen un enfoque más moderno, todavía existen limitaciones en términos de verificación y escalabilidad.

Pero la tecnología Blockchain va más allá de los métodos tradicionales proporcionando un historial descentralizado e inmutable de los registros académicos, así como de las operaciones que respaldan la verificación por parte de terceros, reduciendo gastos, esperas extendidas y mejorando la transparencia en los registros educativos.

## HIPÓTESIS Y JUSTIFICACIÓN

## HIPÓTESIS

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

## JUSTIFICACIÓN

El siguiente proyecto tiene como propósito presentar una propuesta basada en la tecnología Blockchain para instituciones de Educación Superior, específicamente en la certificación de títulos académicos en la Universidad Central del Ecuador. Este tipo de tecnología promete grandes avances en el ámbito de la educación, permitiendo eliminar cuellos de botella en algunos procesos reduciendo los tiempos de espera, además, brinda mayor confianza y transparencia en los registros educativos.

## OBJETIVOS

## OBJETIVO GENERAL

Crear un prototipo de aplicativo web usando tecnología Blockchain para la certificación del idioma inglés en la Facultad de Idiomas de la Universidad Central del Ecuador.

## OBJETIVOS ESPECÍFICOS

- Implementar un modelo para el proceso de certificación de títulos académicos en la Facultad de Ingeniería y Ciencias Aplicadas dentro de la carrera de Sistemas de Información.

- Establecer la herramienta más adecuada para el desarrollo del prototipo.

- Utilizar una metodología ágil para incrementar la flexibilidad del proyecto.

- Realizar una simulación con 30 títulos académicos dentro de la carrera de Sistemas de Información para la validación del modelo.

# 2. MARCO TEÓRICO

**2.1 Conceptos**

**2.1.1Certificación**

El termino 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. Estos pueden ser de distintos tipos, como certificación de empresas, productos y personas.

**2.1.2Certificación 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, como 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.

**2.2 Blockchain**

El termino Blockchain, también conocido como cadena de bloques es una tecnología considerada como disruptiva, que evoluciona periódicamente y ahora es usada por distintas empresas prestigiosas que aprovechan sus características. Esta es considerada una de las principales tecnologías que forman la cuarta revolución industrial.

Blockchain es una red compuesta por varios nodos que contienen registros almacenados en cadenas de bloque. 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 es replicada en cada uno de los nodos, de forma que, si un nodo falla, la red siempre estará activa y disponible.

Esta tecnología permite eliminar la necesidad de un tercero como verificador, por consiguiente, no existe una entidad central que controle los datos; en cambio, la red está compuesta por muchos nodos, que verifican y validan las transacciones. Esto hace que sea muy difícil alterar o modificar la información sin que el resto de la red lo detecte.

**2.2.1 Características de Blockchain**

Estas son algunas características que hacen única a esta tecnología.

**Descentralización**: Los datos en la Blockchain se encuentra almacenados en múltiples nodos de una red, Esto significa que los registros no son controlados por una sola entidad central, lo que reduce riesgos de manipulación o fallas del sistema.

**Inmutabilidad**: es una de las características principales de esta tecnología, Blockchain aplica un sistema por el que el registro de la información se realiza a través de bloques. Una vez que se registra un bloque en la cadena, no puede ser modificado ni eliminado. Esto se debe a que cada bloque contiene un hash criptográfico que lo enlaza con el bloque anterior, formando una cadena de bloques inalterable. Este atributo asegura la integridad y seguridad de la información.

**Disponibilidad**: Los bloques de la cadena se encuentran almacenados en varios nodos dentro de la red. Esto provee alta disponibilidad al momento de acceder a la información porque las transacciones no se encuentran en un solo servidor.

**Transparencia:** Todas las transacciones y datos en una blockchain pública son visibles para todos los participantes en la red. Esto permite verificar y auditar las transacciones, aumentando la confianza entre los usuarios. Cualquiera puede verificar la historia completa de las transacciones realizadas en la cadena.

**Anonimato y Privacidad:** Aunque las transacciones en una blockchain pública son transparentes, los participantes pueden mantener su identidad privada. En lugar de nombres reales, se utilizan direcciones alfanuméricas que representan cada usuario. Sin embargo, existen blockchain privadas que pueden establecer el nivel de anonimato que quiera para realizar o proteger transacciones. Es decir, se puede tener mayor control de identidad y acceso.

**2.2.2 Arquitectura de Blokchain**

Una cadena de bloques es una secuencia de bloques que contiene una lista completa de todos los registros de las transacciones pertenecientes a una red en un libro contable público y abierto.

Diagrama

Descripción generada automáticamente

Figura 1: Estructura blockchain.

La figura 1 ilustra un ejemplo de una cadena de bloques. Con un hash del bloque anterior contenido en la cabecera del bloque, en un bloque solo existe un bloque padre, el único bloque que no contiene un bloque padre es el primer bloque también conocido como bloque génesis.

**2.2.3 Bloque**

Un bloque es un archivo publico que contiene un conjunto de transacciones validadas y replicadas en todos los nodos de una cadena de bloques. Generalmente un bloque se encuentra estructurada en dos partes: la cabecera y el cuerpo.

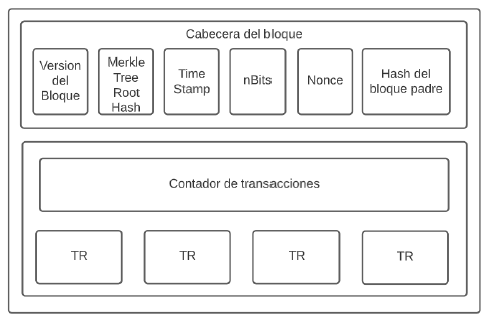


Figura 2. Estructura de un bloque.

Primero la cabecera del bloque, contiene (i) la versión del bloque (también conocido como altura del bloque) indica que conjunto de reglas de validación de bloque se debe seguir, (ii) una marca de tiempo(time Stamp) que indica la fecha exacta en que se formó el bloque, (iii) el tamaño del bloque(medido en bits) que es el umbral de un bloque hash valido, (iv) el nonce, es un numero entero que inicia en cero y va incrementando por cada hash relacionado con el problema matemático asociado a la creación de ese nodo, (v) el hash del bloque padre que es el valor hash de 256 bits que apunta al bloque anterior con excepción del bloque génesis, (vi) raiz del árbol de Merkle es una estructura de datos que contiene hashes criptográficos construidos de abajo hacia arriba, lo que permite resumir y verificar de manera eficiente la integridad de grandes conjuntos de datos.

Segundo el cuerpo del bloque, contiene el libro mayor y un contador de las transacciones que fueron incorporadas en dicho bloque. El número máximo de transacciones que puede contener un bloque depende del tamaño del bloque y del tamaño de cada transacción.

De esta forma, se garantiza la inmutabilidad de las transacciones incluidas en cada bloque, ya que el hash de la raíz de Merkle no coincidiría si se realizara algún cambio en las transacciones.

**2.2.4 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 el fundamento de cualquier blockchain, ya que determinan quién y cómo se genera un nuevo bloque en la cadena. Hay diversos tipos de mecanismos de consenso, a continuación, se detalla algunos de estos.

Prueba de trabajo PoW (Proof of Work): este mecanismo trata de llegar a un acuerdo resolviendo un problema computacionalmente difícil para añadir un nodo a la cadena de bloques.

Prueba de participación PoS (Proof-of-Stake): este mecanismo trata de que los mineros con mas bloques tienen menos probabilidades de atacar la red y con más monedas tendrá la capacidad de producir el siguiente.

Prueba de participación delegada DPoS (Delegated Proof os Stake): consiste en que las partes interesadas de la red eligen al delegado para publicar los bloques y validarlos.

Cualquier mecanismo de consenso debe cumplir con tres criterios fundamentales: validez (asegurar que una transacción válida proviene de un nodo autorizado), conformidad (garantizar que todos los nodos honestos alcancen un consenso respecto al resultado) y terminación (asegurar que todos los nodos legítimos lleguen a una decisión final). Asimismo, estos algoritmos deben incorporar medidas para proteger la seguridad de la blockchain frente a ataques o situaciones críticas.

**2.3 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.

**Estructura**

Un contrato inteligente consta del valor, la dirección, las funciones y el estado. Toma

la transacción como datos de entrada, ejecuta el código correspondiente y activa los eventos de salida. Dependiendo de la lógica de la función, los estados de implementación cambian.

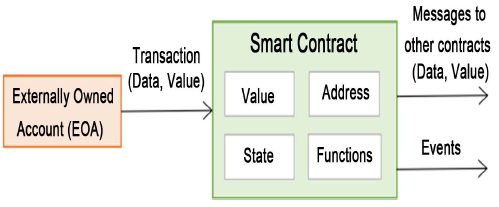


Figura 3. Estructura básica de un contrato inteligente.

**Ethereum y EVM**

Ethereum es una plataforma digital descentralizada y de código abierto que utiliza la tecnología blockchain, brindando a los desarrolladores la posibilidad de diseñar y ejecutar contratos inteligentes. Esto permite aprovechar al máximo las ventajas de la tecnología blockchain.

En el apartado anterior, se introdujo el concepto de blockchain junto con sus principales características y elementos fundamentales. En este segmento, se detallarán los componentes específicos de Ethereum, incluyendo su estructura interna y el contenido de sus bloques.

Ethereum opera con dos tipos de cuentas:

1. Cuentas externas: controladas mediante claves privadas.
2. Cuentas de contratos: gestionadas por el código del contrato.

Ambas cuentas tienen direcciones de 20 bytes y soportan cambios de estado. Los campos de las cuentas incluyen:

* Nonce: un contador que garantiza que cada transacción sea procesada una sola vez.
* Saldo: la cantidad de Ether asociada a la cuenta.
* Código del contrato: solo presente en cuentas de contratos.
* Almacenamiento: datos específicos de la cuenta.

A diferencia de Bitcoin, Ethereum es Turing completo, lo que significa que puede ejecutar programas de cualquier complejidad. Sin embargo, esto puede generar problemas de saturación en la red. Para mitigar este inconveniente, Ethereum utiliza un mecanismo denominado *gas*. Cada instrucción ejecutada por la Ethereum Virtual Machine (EVM) tiene un coste de gas, y para realizar transacciones o ejecutar contratos, se debe asignar un límite máximo de gas. El gas, que se compra con Ether, regula el consumo computacional y asegura la sostenibilidad de la red.

El Ether, es la criptomoneda nativa de Ethereum se emplea como medio de pago en las transacciones. Durante cada transacción, se debe incluir una cantidad específica de Ether destinada al pago del gas.

**Solidity**

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

Algunas características que distinguen a Solidity son:

Lenguaje orientado a objetos: Solidity emplea los principios de la programación orientada a objetos, como el uso de clases para crear objetos que interactúan entre sí. Esto facilita la creación de código reutilizable y de fácil mantenimiento.

Tipado estático: Los tipos de datos en Solidity deben declararse durante la compilación, y una vez definido el tipo de una variable, este no puede ser modificado. Solo es posible cambiar el valor de la variable si pertenece al mismo tipo. Esta propiedad ayuda a identificar errores relacionados con los tipos de datos durante la fase de desarrollo, evitando problemas en la ejecución.

Curva de aprendizaje baja: La sintaxis de Solidity es similar a la de JavaScript, lo que facilita su comprensión para desarrolladores con experiencia en este u otros lenguajes backend como Java o .NET. Además, la programación orientada a objetos proporciona una transición sencilla para programadores familiarizados con estas herramientas. El lenguaje cuenta con buena documentación y requiere únicamente una comprensión básica de su entorno para comenzar a trabajar.

Optimizado para la EVM: Solidity está diseñado específicamente para Ethereum y su Ethereum Virtual Machine (EVM). Su objetivo principal es proporcionar una forma simple y eficiente de desarrollar contratos inteligentes que aprovechen al máximo las capacidades de la EVM.

# Metodología experimental

# Cálculos y resultados

# Discusión de resultados

# Conclusiones

# Recomendaciones

# Bibliografía

# Anexos