MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE GRADUACIÓN

Sometido al Tribunal Examinador de Postgrados para optar por el grado de Maestría en Ciberseguridad

“Propuesta de la arquitectura tecnológica para un sistema de validación de Certificados Académicos basado en Blockchain para la prevención del fraude en la Universidad Internacional San Isidro Labrador durante el periodo lectivo 2025”

AUTOR

Ing. Guillermo Mora Granados

TUTOR: MsC. Randall Artavia Delgado

LECTOR: Ing. Irvin Argenis Sáenz Cordoba

Pérez Zeledón, Costa Rica

Diciembre, 2025

UNIVERSIDAD SAN ISIDRO DEL LABRADOR
MAESTRÍA EN CIBERSEGURIDAD

TRIBUNAL EXAMINADOR

Ruddy RA

Ing. Ruddy Rodriguez Acuña
Director de Maestría

Msc. Randall Artavia Delgado
Tutor

Ing. Irvin Argenis Sáez Cordoba
Lector

DECLARACIÓN JURADA

Yo, Guillermo Mora Granados, mayor, unión libre, egresado(a) de la carrera de Maestría Profesional en Ciberseguridad de la Universidad San Isidro Labrador, domiciliado en la ciudad de San Isidro, Pérez Zeledón, portador(a) de la cédula de identidad número 1-1306-0863, en este acto, debidamente apercibido y entendido de las penas y consecuencias con las que se castiga, en el Código Penal, el delito del perjurio, ante quienes se constituyen en el Tribunal Examinador de mi Trabajo Final de Graduación para optar por el título de maestría, juro solemnemente que mi trabajo final de graduación titulado **"Propuesta de la arquitectura tecnológica para un sistema de validación de Certificados Académicos basado en Blockchain para la prevención del fraude en la Universidad Internacional San Isidro Labrador durante el periodo lectivo 2025"** es una obra original que ha respetado todo lo preceptuado por las Leyes Penales así con la Ley de Derechos de Autor y Derechos Conexos, número 6683 de 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 de 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte: artículo 70°: Es permitido citar a un autor transcribiendo los pasajes pertinentes siempre que estos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor y de la obra original. Asimismo, quedo advertido que la Universidad San Isidro Labrador se reserva el derecho de protocolizar este documento ante Notario Público. En fe de lo anterior firmo en la ciudad de San Isidro, al ser el 06 del mes de diciembre del año dos mil veinticinco.

Guillermo Mora Granados
Cédula: 1-1306-0863

DEDICATORIA

A mi familia que son mi impulso para desear ser mejor cada día. A Cindy, Yael, mis padres y mi hermano que están ahí siempre creyendo en mí.

AGRADECIMIENTOS

A Dios en primer lugar, por darme la sabiduría y la fuerza para cumplir con los proyectos que me he propuesto.

A los profesores de la Maestría, que ha sabido comunicar y compartir su conocimiento con todos nosotros.

Al profe Randall por su acompañamiento en este proceso de elaboración del proyecto.

Al profe Irvin, que se ha preocupado por darnos un poco más del contenido del curso y ayudarnos a crecer un poco más profesionalmente.

A todas las personas que de una u otra forma colaboraron para que este proyecto se pudiera realizar.

CARTA DE AUTORIZACIÓN DEL TUTOR

Pérez Zeledón, 06 de diciembre del 2025

Licenciado
Ruddy Rodríguez Acuña
Coordinador de la Escuela de Informática
Universidad Internacional San Isidro Labrador

Estimado señor Coordinador:

Yo, Randall Mauricio Artavia Delgado, mayor, Ingeniero en informática, con domicilio en la Trinidad de Moravia San José, portador de la cédula de identidad número **205740823**, en mi condición de tutor del Proyecto de Graduación titulado **"Propuesta de la arquitectura tecnológica para un sistema de validación de Certificados Académicos basado en Blockchain para la prevención del fraude en la Universidad Internacional San Isidro Labrador durante el periodo lectivo 2025"** propuesto por el estudiante **Guillermo Mora Granados**, manifiesto lo siguiente:

1. Que el proceso de trabajo final de graduación culmina satisfactoriamente.
2. Que se ha incorporado en el documento final las sugerencias hechas por el Tribunal Examinador.
3. Que he cumplido con el acompañamiento encomendado por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,

MATI Randall Mauricio Artavia Delgado
Tutor

CARTA DE APROBACIÓN DEL LECTOR

Pérez Zeledón, 06 de diciembre del 2025

Licenciado
Ruddy Rodríguez Acuña
Coordinador de la Escuela de Informática
Universidad Internacional San Isidro Labrador

Estimado señor Coordinador:

Yo, Irvin Argenis Saenz Cordoba, mayor, casado, Analista de Ciberseguridad, vecino de Guápiles, portador de la cédula de identidad número **701970839**, en mi condición de lector del Proyecto de Graduación titulado **"Propuesta de la arquitectura tecnológica para un sistema de validación de Certificados Académicos basado en Blockchain para la prevención del fraude en la Universidad Internacional San Isidro Labrador durante el periodo lectivo 2025"** propuesto por el estudiante **Guillermo Mora Granados**, manifiesto lo siguiente:

1. Que la lectura del trabajo final de graduación concluye satisfactoriamente.
2. Que he leído el documento final y he hecho mis observaciones en el mismo.
3. Que he cumplido con las labores de lector encomendadas por la Universidad en forma y fondo.
4. Que considero que el documento final responde a las exigencias académicas establecidas por la Universidad.

Atentamente,

Máster Irvin Argenis Saenz Cordoba
Lector

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS Y CUADROS

ÍNDICE DE GRÁFICOS, FIGURAS E ILUSTRACIONES

LISTA DE PALABRAS CLAVES

Blockhain, Smart Contract, Criptografía, Descentralización, Inmutabilidad, Certificados académicos, Validación de certificados, Prevención de fraude, Autenticidad, Transparencia, Credenciales, Tokens, Hashing, Cadena de bloques, Trazabilidad, Auditoría, Falsificación, Proof of work, Bloque, Sistema de validación, Arquitectura tecnológica

RESUMEN EJECUTIVO

Este documento presenta la propuesta de una arquitectura tecnológica orientada a implementar un sistema de validación de certificados académicos basado en la tecnología Blockchain en la Universidad Internacional San Isidro Labrador (UISIL) para el año lectivo 2025, con el objetivo primordial de prevenir el fraude y la falsificación de títulos. El problema central identificado es la vulnerabilidad y la ineficiencia de los procesos actuales de emisión y verificación, que dependen de documentos físicos y procesos manuales, generando una carga administrativa y retrasos considerables en la verificación por parte de terceros.

La propuesta arquitectónica se centra en integrar un Módulo de Emisión en Blockchain con el Sistema de Gestión de Procesos (ERP) existente de la universidad. Esta solución aprovecha la inmutabilidad, la trazabilidad y la naturaleza descentralizada de Blockchain para garantizar la autenticidad irrefutable de cada credencial emitida. El estudio de viabilidad técnica determinó que HyperLedger es la plataforma *blockchain* más adecuada para el entorno universitario. El diseño del sistema contempla la inclusión de un código QR en el certificado en formato PDF, el cual, al ser escaneado por cualquier tercero (como empleadores), redirige a una plataforma de validación que consulta instantáneamente el registro de autenticidad en la cadena de bloques.

Los resultados del diagnóstico confirmaron la necesidad crítica de esta solución, mostrando una alta preocupación por el fraude por parte de las autoridades académicas. Más importante aún, la encuesta a empleadores reveló que consideran el proceso de verificación actual como crítico o lento, y manifestaron una aceptación total a adoptar una solución basada en Blockchain para una validación segura e instantánea. En resumen, si bien este proyecto es una propuesta de diseño conceptual y teórica y no una implementación operativa, proporciona la hoja de ruta para que la UISIL modernice su gestión de títulos, reduzca costos administrativos, empodere a los estudiantes con credenciales seguras y ofrezca a empleadores un mecanismo de verificación instantáneo y totalmente confiable.

CAPITULO I. INTRODUCCIÓN

1.1 Planteamiento del tema de estudio

Los **sistemas actuales de emisión y validación de certificados académicos en la Universidad Internacional San Isidro Labrador presentan deficiencias significativas** que se manifiestan en varios problemas críticos. Principalmente, existe una **alta vulnerabilidad al fraude y la falsificación.** La emisión de certificados en formato físico (papel) y la dependencia de procesos manuales facilitan la manipulación de certificados, la creación de certificados fraudulentos por externos a la universidad y la suplantación de identidad. Esta debilidad compromete la confianza en la validez de los títulos y cursos impartidos por la universidad, afectando negativamente su prestigio y el de sus egresados en el ámbito laboral y profesional.

En segundo lugar, los **procesos actuales son ineficientes y generan una carga administrativa considerable.** La emisión de certificados implica costos de impresión, sellado y firma, así como el tiempo y la logística asociados al retiro físico de los documentos por parte de los estudiantes. Asimismo, la verificación de la autenticidad de estos certificados por parte de empleadores o instituciones educativas externas es un proceso lento y a menudo requiere una comunicación directa y demorada con la universidad, lo que ralentiza los procesos de contratación o admisión.

La situación actual de la universidad, que emite certificados físicos y digitales carentes de un sistema de validación robusto, expone a la institución a los riesgos y desafíos que la literatura especializada en blockchain ha identificado. La falta de un mecanismo de validación seguro hace que los certificados emitidos sean vulnerables a la falsificación y al fraude, un problema que los autores Al-Ma'ani et al. (2024) y Bapat (2020) señalan como una debilidad de los sistemas tradicionales.

En este contexto, la implementación de una solución basada en blockchain no solo respondería a la necesidad de la universidad de garantizar la autenticidad de sus certificados, sino que también la alinearía con la visión de los autores. Por ejemplo, la tecnología propuesta por Sharma y Gupta (2024), que utiliza un registro

inalterable para reducir el fraude, se presenta como una alternativa directa al problema de falsificación. De manera similar, la solución descentralizada de Taylor & Francis (2025) y la automatización de la verificación a través de contratos inteligentes que mencionan Al-Ma'ani et al. (2024), resolverían la carga administrativa que enfrentan los verificadores y la propia universidad, permitiendo que el proceso sea más eficiente y menos costoso.

Finalmente, los estudiantes carecen de un **control directo y eficiente sobre sus propios títulos.** Los certificados de papel pueden perderse, dañarse o deteriorarse con el tiempo, y su compartición con terceros es un proceso manual y a menudo lento. Esta falta de autonomía y agilidad en la gestión de sus logros académicos limita la capacidad de los estudiantes para presentar sus calificaciones de manera oportuna y segura. En este contexto, surge la necesidad de un sistema que garantice la autenticidad, la inmutabilidad y la accesibilidad de los certificados, combatiendo el fraude, optimizando los procesos operativos y brindando a los estudiantes una mayor autonomía sobre sus certificados académicos.

1.2 Antecedentes del tema

Históricamente, la emisión y gestión de certificados académicos ha dependido en gran medida de **procesos manuales y formatos físicos**, predominando el uso de documentos impresos, como diplomas, transcripciones de calificaciones y constancias. Estos certificados se validan mediante elementos como sellos, firmas autógrafas y papel de seguridad, y su autenticidad se ha verificado tradicionalmente a través de procesos administrativos que implican la comunicación directa con la institución emisora. La Universidad Internacional San Isidro Labrador, como muchas otras instituciones educativas, ha seguido este modelo operativo para la expedición de sus certificados (Universidad Internacional San Isidro Labrador, 2025). Este enfoque, si bien ha sido la norma durante décadas, ha propiciado la aparición y persistencia de una serie de vulnerabilidades significativas.

Una de las principales debilidades de los sistemas de certificación tradicionales es su **alta susceptibilidad al fraude y la falsificación**. Los documentos físicos son inherentemente vulnerables a la alteración, ya sea mediante la modificación de calificaciones, la creación de diplomas completamente falsos o la suplantación de identidad. El fraude académico abarca diversas prácticas, desde la falsificación de documentos hasta el soborno para alterar registros, todas las cuales socavan la integridad del sistema educativo y la confianza en los certificados emitidos (Acreditta, n.d.).

Estas actividades fraudulentas no solo comprometen la validez de los logros académicos y la reputación de los egresados, sino que también pueden tener un impacto económico considerable para las instituciones y para las empresas que contratan personal con base en certificados falsos. La prevalencia de este tipo de problemas ha generado una preocupación creciente en el ámbito educativo global, impulsando la búsqueda de soluciones más robustas y seguras para la autenticación de certificados (Acreditta, n.d.).

Además de la vulnerabilidad al fraude, los procesos tradicionales de certificación son **ineficientes y generadores de costos operativos significativos**. La impresión, el sellado y la firma manual de grandes volúmenes de certificados representan una carga administrativa considerable en términos de tiempo, recursos materiales y personal. Para los estudiantes, el retiro físico de sus certificados en las instalaciones universitarias implica desplazamientos y esperas, lo que puede ser un inconveniente considerable. De igual forma, la verificación de la autenticidad de un certificado por parte de terceros (como empleadores o instituciones de posgrado) es un proceso que a menudo requiere contactar directamente a la universidad, lo que consume tiempo y retrasa los procesos de contratación o admisión. Esta situación ha puesto de manifiesto la necesidad de innovar en la gestión de certificados, buscando alternativas que no solo refuercen la seguridad, sino que también optimicen la eficiencia operativa y mejoren la experiencia tanto para la universidad como para los usuarios de los certificados.

Varios autores destacan que la naturaleza descentralizada e inmutable de blockchain es ideal para combatir el fraude de certificados. Almacenar un "hash" del certificado digital en una cadena de bloques asegura que, una vez registrado, el documento no puede ser alterado sin ser detectado.

- "La tecnología blockchain ofrece un entorno seguro donde cada credencial se almacena y recupera de manera segura, proporcionando un registro inalterable que reduce significativamente la posibilidad de fraude" (Sharma & Gupta, 2024, p. 2).
- "La inmutabilidad de los registros de blockchain garantiza que, una vez que se genera una credencial, no se puede alterar, eliminar o manipular, lo que asegura un nivel muy alto de seguridad y confianza" (Patel, 2023, p. 2).
- "La implementación de un sistema de validación de certificados utilizando la tecnología blockchain arrojó varios resultados significativos, demostrando la eficacia y fiabilidad del sistema. En primer lugar, la solución basada en blockchain aseguró con éxito la inmutabilidad y seguridad de los certificados. Una vez que se emitió un certificado y se registró su hash correspondiente en la cadena de bloques, se volvió virtualmente imposible alterar el certificado sin ser detectado" (Musa et al., 2024, p. 5).

Por otra parte, con respecto a la reducción de carga administrativa de la cual se pueden ver beneficiados los funcionarios de la Universidad Internacional San Isidro labrador, Taylor & Francis, 2025, p. 1. indican que "Al descentralizar el proceso, el sistema propuesto elimina la necesidad de autoridades centralizadas, lo que garantiza una mayor transparencia, seguridad y confianza en el proceso de verificación. El sistema también simplifica el acceso tanto para las instituciones como para los empleadores, mejorando la eficiencia y reduciendo los costos"

1.3 Justificación

La implementación de un sistema de validación de certificados académicos basado en la tecnología blockchain es un paso importante y estratégico para la Universidad Internacional San Isidro Labrador. Esta iniciativa responde directamente a la urgente necesidad de combatir el fraude académico, un problema que socava la credibilidad de los diplomas y pone en riesgo la reputación de la institución. Al pasar de un sistema vulnerable, manual y dependiente de documentos físicos a una solución digital y descentralizada, se eliminará la posibilidad de falsificación y se garantizará la inmutabilidad de los logros académicos.

La implementación de un sistema de validación de certificados académicos basado en la tecnología blockchain es un paso crucial y estratégico para la Universidad Internacional San Isidro Labrador. Esta iniciativa responde directamente a la urgente necesidad de combatir el fraude académico, un problema que socava la credibilidad de los diplomas y pone en riesgo la reputación de la institución. Al pasar de un sistema vulnerable, manual y dependiente de documentos físicos a una solución digital y descentralizada, se eliminará la posibilidad de falsificación y se garantizará la inmutabilidad de los logros académicos.

¿Por qué es importante y quiénes son los beneficiarios?

La importancia de este trabajo reside en su capacidad para transformar la gestión de credenciales académicas, beneficiando a múltiples actores:

La Universidad: Fortalecerá su imagen y reputación al posicionarse como una institución a la vanguardia tecnológica, comprometida con la seguridad y la transparencia. Al reducir los procesos manuales, la universidad experimentará una reducción de costos y una mayor eficiencia en la emisión y verificación de

certificados. Esto se alinea directamente con su visión de ser una entidad proactiva y tecnológicamente avanzada.

Los Estudiantes: Serán los principales beneficiarios al obtener control total sobre sus certificados. La tecnología blockchain les permitirá compartir sus credenciales de forma segura, instantánea y sin intermediarios con empleadores o instituciones educativas. Esto les otorgará un mayor empoderamiento y autonomía sobre su trayectoria académica, facilitando su inserción en un mercado laboral cada vez más competitivo.

Los Empleadores y Otras Instituciones: Se beneficiarán de un sistema de verificación instantánea y confiable. Ya no tendrán que contactar a la universidad para validar un diploma, lo que agilizará los procesos de contratación y selección, mejorando la confianza en las credenciales de los egresados de la Universidad San Isidro Labrador.

¿Qué se pretende cambiar y cuál es su utilidad?

El proyecto tiene como objetivo cambiar el paradigma de la certificación académica. Se pasará de un modelo ineficiente y susceptible de fraude a un sistema moderno, seguro y transparente. La utilidad de esta iniciativa es doble, en primera instancia, proporciona un método infalible para la autenticación de certificados, eliminando las debilidades de los sistemas actuales y en segundo lugar, contribuye a la misión de la universidad de formar profesionales competentes, asegurando que sus logros educativos sean reconocidos y valorados con la máxima integridad.

Este proyecto es significativo, no solo propone una solución tecnológica, sino que también sirve como un modelo de innovación educativa para otras instituciones. Aporta una propuesta metodológica clara para la integración de blockchain en un contexto académico real. La investigación proveerá un marco de trabajo que combina teoría y práctica, demostrando cómo una tecnología emergente puede ser aplicada para resolver problemas concretos de gestión universitaria.

La tecnología blockchain ofrece una solución robusta a estos desafíos al proporcionar un **registro inmutable, seguro y transparente de las certificados.** Esto significa que una vez que un certificado es emitido en la red de blockchain, su autenticidad e integridad no pueden ser alteradas, eliminando prácticamente la posibilidad de fraude. Al mismo tiempo, empodera al estudiante al darle **control total sobre sus certificaciones,** permitiéndoles compartirlas de manera segura y eficiente con terceros sin necesidad de intermediarios. Esta propuesta no solo modernizará el proceso de emisión de certificados de la Universidad Internacional San Isidro Labrador, sino que también la posicionará a la vanguardia tecnológica, reforzando su compromiso con la excelencia académica y la seguridad de sus procesos en cumplimiento tanto de su misión como de su visión.

Misión:

"Somos una Universidad que promueve y contribuye con la formación de líderes profesionales y técnicos con capacidad crítica, de investigación y análisis que respondan a los desafíos y necesidades del desarrollo del país; en especial de los sectores sociales más excluidos de la educación superior por razones de distancia y condiciones socioeconómicas, mediante un modelo de Universidad integrada, que brinda opciones para el mejoramiento de la calidad de vida de sus estudiantes, familias y comunidades donde tiene influencia."

Visión:

"Ser una Universidad proactiva, reconocida por su capacidad para dar respuesta a los desafíos y a las demandas de un entorno cambiante, a la vanguardia tecnológica y con un espíritu humanista, que contribuye al desarrollo local, regional, nacional e internacional; mediante el compromiso de ser un ente generador de conocimiento, cultura e investigación y que prepara a sus estudiantes con excelencia académica profesional y tecnológica para insertarse en un mercado laboral altamente competitivo."

1.4 Objetivos

1.4.1 Objetivo general

Desarrollar una propuesta del diseño arquitectónico tecnológico para un sistema de validación de certificados académicos basado en tecnología blockchain para la prevención del fraude en la Universidad Internacional San Isidro Labrador durante el periodo lectivo 2025.

1.4.2 Objetivos específicos

1. Diagnosticar la situación actual respecto a la arquitectura tecnológica de la emisión de certificados académicos en la Universidad Internacional San Isidro Labrador.

2. Realizar un estudio de viabilidad técnica y un análisis comparativo de plataformas blockchain, seleccionando la más adecuada y justificando su elección para un futuro prototipo o implementación en un entorno universitario.

3. Diseñar la arquitectura tecnológica de un sistema de emisión y validación de certificados universitarios que utilice blockchain para asegurar la inmutabilidad y autenticidad de los certificados, previniendo la falsificación y el fraude.

1.5 Alcances

Este proyecto se enfoca en la etapa de definición y planificación de un sistema de validación de títulos universitarios utilizando tecnología blockchain. El ámbito de estudio es la Universidad Internacional San Isidro Labrador, Sede Central, ubicada en Pérez Zeledón, y se ejecutará durante el año 2025. El objetivo

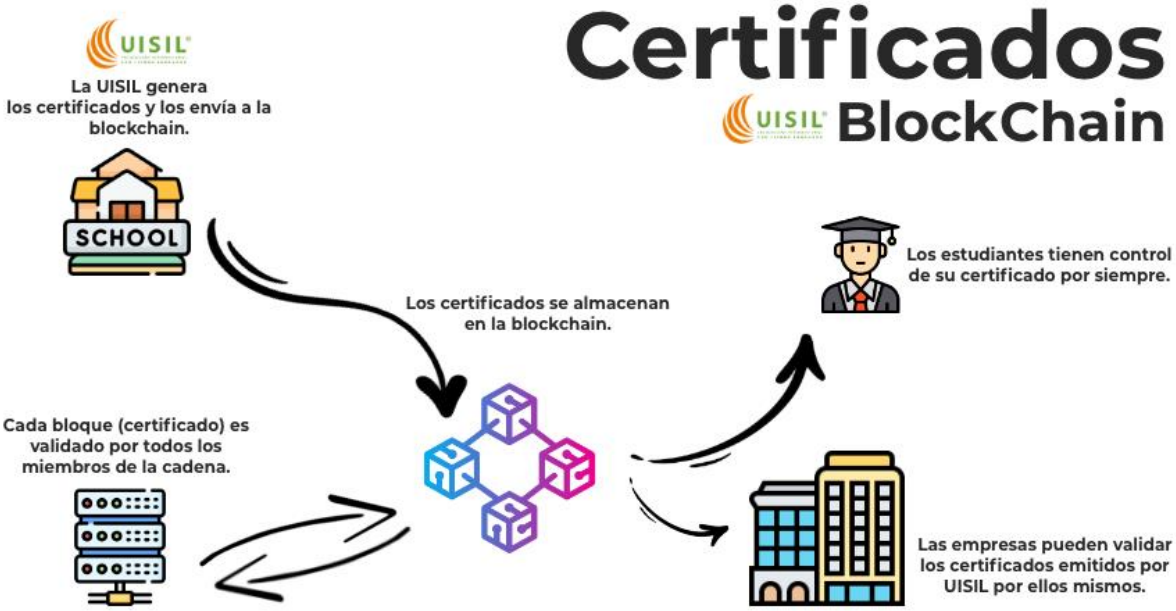
principal es sentar las bases conceptuales y funcionales para un futuro sistema que modernice la emisión y verificación de certificados académicos, garantizando su integridad y autenticidad.

Actualmente, la universidad utiliza un Sistema de Gestión de Procesos que permite a los colaboradores del Centro de Extensión Universitaria (CEU) emitir certificados de forma digital. La propuesta de este proyecto es complementar esta funcionalidad mediante el diseño de un módulo adicional que integre los certificados emitidos con una red blockchain. Este nuevo módulo tendrá como propósito principal registrar la huella digital de cada certificado en la cadena de bloques, creando un registro inmutable y verificable.

El diseño del nuevo módulo también incluirá una interfaz de usuario de validación con estrictos protocolos de protección de datos personales. Esto asegurará que solo las entidades autorizadas puedan consultar la autenticidad de los certificados. La verificación se facilitará a través de la incorporación de un código QR en el certificado en formato PDF. Al escanear este código, los usuarios serán redirigidos a una plataforma que verificará la validez del documento directamente en la blockchain, eliminando la necesidad de intermediarios y agilizando el proceso.

Es fundamental destacar que el alcance de este proyecto se limita a la etapa de definición y planificación. No se contempla el desarrollo, la implementación ni la puesta en marcha de la solución final. Tampoco se buscará la obtención de resultados finales medibles ni la implementación de las estrategias propuestas. Este enfoque metodológico permitirá estructurar un marco sólido que servirá como hoja de ruta para futuros proyectos de desarrollo e implementación, garantizando una transición exitosa hacia una gestión de certificados más segura y eficiente.

Figura 1: Alcance del proyecto



Nota: Elaboración propia

Elaborado por Ing. Guillermo Mora Granados

1.6 Limitaciones

El proyecto se limita a ser una propuesta de diseño arquitectónico, no la implementación o desarrollo de un sistema funcional. Su alcance se restringe a la etapa de "definición y planificación", lo que significa que este proyecto es de carácter conceptual y teórico. Esto implica que el proyecto no generará una solución operativa ni un prototipo tangible, sino que sentará las bases y proporcionará una hoja de ruta para que futuras iniciativas puedan llevar a cabo la implementación.

Una limitación directa de este enfoque es la ausencia de una validación empírica y resultados medibles. Dado que el proyecto no contempla la implementación, no se podrá demostrar de manera práctica la efectividad de la arquitectura propuesta en la prevención del fraude o en la mejora de la eficiencia. La viabilidad y el éxito de la solución, tal como se plantea, se basan en un análisis teórico y comparativo, sin que se pueda obtener una evidencia tangible de su funcionamiento en un entorno real.

El alcance geográfico y organizacional del proyecto es una limitación significativa, ya que se centra exclusivamente en el contexto de la Universidad Internacional San Isidro Labrador, Sede Central. Esto restringe la generalización de los hallazgos y de la arquitectura propuesta a otras instituciones educativas. Las necesidades y los procesos específicos de esta universidad, así como su infraestructura tecnológica actual, podrían no ser representativos de otras instituciones, haciendo que la propuesta sea un estudio de caso muy particular.

Finalmente, la viabilidad técnica y económica del proyecto enfrenta limitaciones importantes. Si bien se plantea un estudio de viabilidad , el documento ya identifica el presupuesto y los costos considerables de ciertas plataformas blockchain como Ethereum como una de las principales restricciones y riesgos. Esto sugiere que la implementación de la propuesta podría enfrentar obstáculos financieros y técnicos que no serán resueltos dentro del alcance de este proyecto de definición.

1.7 Cronograma de actividades

ID	Tarea	Inicio	Fin	Duración
1	Fase I: Diagnóstico y Revisión Teórica (Septiembre)	01/09/2025	03/10/2025	25 días
2	1.1. Revisión de literatura sobre blockchain y certificaciones.	01/09/2025	09/09/2025	7 días
3	1.2. Mapeo del proceso de emisión de certificados actual.	05/09/2025	16/09/2025	8 días
4	1.3. Preparación de instrumentos para entrevistas y encuestas.	15/09/2025	23/09/2025	7 días
5	1.4. Identificación de sujetos de información clave (CEU, Registro, Gerencia).	25/09/2025	03/10/2025	7 días
6	Fase II: Recolección y Análisis de Datos (Octubre)	06/10/2025	31/10/2025	20 días
7	2.1. Aplicación de entrevistas a profundidad con el personal de la universidad.	06/10/2025	17/10/2025	10 días
8	2.2. Aplicación de encuestas a empresas para conocer sus necesidades de verificación.	09/10/2025	22/10/2025	10 días
9	2.3. Transcripción y análisis de los datos cualitativos de las entrevistas.	23/10/2025	24/10/2025	2 días
10	2.4. Análisis de los resultados de las encuestas a empresas.	27/10/2025	31/10/2025	5 días
11	Fase III: Estudio de Viabilidad y Comparativa de Plataformas (Noviembre)	03/11/2025	19/11/2025	13 días
12	3.1. Investigación de plataformas blockchain (Ethereum, Solana, Hyperledger).	03/11/2025	11/11/2025	7 días
13	3.2. Creación de una matriz de análisis comparativo de las plataformas.	11/11/2025	14/11/2025	4 días
14	3.3. Justificación y selección de la plataforma blockchain más adecuada.	14/11/2025	18/11/2025	3 días
15	3.4. Redacción del informe de viabilidad técnica y comparativa.	18/11/2025	19/11/2025	2 días
16	Fase IV: Diseño de la Arquitectura y Documentación (Diciembre)	21/11/2025	04/12/2025	10 días
17	4.1. Diseño conceptual del módulo de emisión de certificados en blockchain.	21/11/2025	25/11/2025	3 días
20	4.2. Diseño de la interfaz de usuario de validación (usando códigos QR).	24/11/2025	26/11/2025	3 días

21	4.3. Desarrollo de un protocolo de protección de datos.	26/11/2025	01/12/2025	4 días
19	4.4. Redacción final del documento de la propuesta de diseño arquitectónico.	01/12/2025	03/12/2025	3 días
18	4.5. Presentación de la propuesta de diseño a las partes interesadas.	06/12/2025	04/12/2025	1 día

1.8 Producto esperado del TFG

Objetivos específicos	Entregables	Formato
1. Diagnosticar la situación actual respecto a la arquitectura tecnológica de la emisión de certificados académicos en la Universidad Internacional San Isidro Labrador.	Diagnóstico de la situación actual de las tecnologías de emisión de certificados académicos en la UISIL.	PDF
4. Realizar un estudio de viabilidad técnica y un análisis comparativo de plataformas blockchain, seleccionando la más adecuada y justificando su elección para un futuro prototipo o implementación en un entorno universitario.	Estudio de viabilidad técnica y análisis comparativo de plataformas blockchain.	PDF
5. Diseñar la arquitectura tecnológica de un sistema de emisión y validación de certificados universitarios que utilice blockchain para asegurar la inmutabilidad y autenticidad de los certificados, previniendo la falsificación y el fraude.	Diseño de la arquitectura del sistema de emisión y validación de certificados universitarios.	PDF

CAPÍTULO II. MARCO TEÓRICO

El presente marco teórico aborda los fundamentos de la tecnología **blockchain** y su aplicación específica en la **certificación académica**, explorando cómo sus características intrínsecas ofrecen una solución robusta a las deficiencias de los sistemas tradicionales. Se estructura a partir de conceptos clave que justifican su adopción como una herramienta de vanguardia para la emisión y validación de credenciales educativas.

1. Fundamentos de la Tecnología Blockchain

La blockchain, o cadena de bloques, es una tecnología que ha emergido como una de las innovaciones más disruptivas del siglo XXI. A su esencia, es un tipo de libro de contabilidad distribuido (DLT) en el que se registran transacciones de forma segura y transparente. A diferencia de las bases de datos tradicionales, la blockchain se caracteriza por una arquitectura descentralizada y una estructura de datos secuencial e inmutable. Grant Thornton (s.f.) la define como "un registro digital distribuido en el que se plasman datos de manera secuencial y permanente en forma de 'bloques'". Cada bloque nuevo se enlaza criptográficamente al anterior, formando así la cadena. Esta estructura no solo asegura la integridad de los datos, sino que también elimina la necesidad de intermediarios, lo que la convierte en una tecnología de confianza (Preukschat, 2017).

Con respecto al blockchain, podríamos decir lo siguiente:

- Blockchain es un tipo de base de datos compartida que se diferencia de una base de datos típica en la forma en que almacena información; las cadenas de bloques almacenan datos en bloques vinculados entre sí mediante criptografía.
- Se pueden almacenar diferentes tipos de información en una cadena de bloques, pero el uso más común ha sido como libro de contabilidad de transacciones.
- En el caso de Bitcoin, la cadena de bloques está descentralizada, por lo que ninguna persona o grupo tiene el control —en cambio, todos los usuarios conservan el control colectivamente.

- Las cadenas de bloques descentralizadas son inmutables, lo que significa que los datos ingresados son irreversibles. En el caso de Bitcoin, las transacciones se registran de forma permanente y cualquier persona puede verlas.

¿Cómo funciona una cadena de bloques?

Una cadena de bloques consta de programas llamados scripts que realizan las tareas que normalmente realizaría en una base de datos: ingresar y acceder a información, y guardarlo y almacenarlo en algún lugar. Se distribuye una cadena de bloques, lo que significa que se guardan varias copias en muchas máquinas y todas deben coincidir para que sea válida.

La cadena de bloques de Bitcoin recopila información de transacciones y la ingresa en un archivo de 4 MB llamado bloque (diferentes cadenas de bloques tienen bloques de diferentes tamaños). Una vez que el bloque está lleno, los datos del bloque se ejecutan a través de una función hash criptográfica, que crea un número hexadecimal llamado encabezado de bloque hash.

Luego, el hash se ingresa en el siguiente encabezado de bloque y se cifra con la otra información en el encabezado de ese bloque, creando una cadena de bloques, de ahí el nombre “blockchain”

Proceso de transacción

El proceso de registro de información en una blockchain se fundamenta en un sistema de transacciones que sigue una secuencia de eventos específica, la cual varía ligeramente dependiendo de la arquitectura de la red.

Aunque el ejemplo clásico es Bitcoin, donde las transacciones son transferencias de valor, en plataformas como Ethereum o Solana, una transacción puede ser la ejecución de un contrato inteligente que registra un certificado. Para un usuario, el proceso se inicia a través de una billetera de criptomonedas o una aplicación descentralizada (dApp), que actúa como la interfaz para interactuar con la cadena de

bloques. Esta interfaz es la puerta de entrada para iniciar la secuencia de eventos que culminará en un registro inmutable.

En el contexto de la certificación académica, el proceso de transacción en la blockchain no implica la minería de Bitcoin, sino que se adapta a las reglas de la plataforma elegida, como Ethereum o Solana. Para emitir un certificado, la universidad, a través de su dApp, inicia una transacción en la que se ejecuta un contrato inteligente.

Esta transacción no transfiere valor monetario, sino que lleva consigo datos importantes: el hash criptográfico del certificado digital, la fecha de emisión y la firma digital de la universidad. Esta transacción se envía a un grupo de memoria de la red, donde espera ser procesada.

A continuación, la transacción es recogida por un validador (en redes de prueba de participación como Ethereum y Solana) o un minero (en redes de prueba de trabajo), que se encarga de agruparla con otras transacciones en un bloque. Una vez que el validador verifica la transacción, el bloque se cierra, se sella criptográficamente y se añade a la cadena de bloques existente. El proceso, que puede durar desde unos pocos segundos hasta varios minutos según la red, finaliza cuando el bloque es validado por la mayoría de los nodos de la red. En ese momento, el registro del certificado se vuelve inmutable y públicamente verificable, lo que lo hace a prueba de manipulaciones.

Este proceso de transacción, adaptado a la emisión de certificados, es lo que permite que la tecnología blockchain sea una solución tan efectiva. Al igual que en el modelo descrito por Nakamoto (s.f.) para las transacciones financieras, cada registro de certificado es validado por la red de manera descentralizada, garantizando que el origen y la integridad del documento sean incuestionables.

Una vez que la transacción del certificado ha sido confirmada y añadida a un bloque, cualquier persona puede verificar su autenticidad sin necesidad de recurrir a la universidad, simplemente utilizando el hash del documento y consultando la cadena de bloques.

1.2. Bloque (Block): La Unidad Básica

El **bloque** es la unidad fundamental de una blockchain. Cada bloque es un contenedor de información que incluye:

- **Datos de la Transacción:** La información relevante del registro. En el caso de los certificados académicos, esto podría ser el nombre del estudiante, el título obtenido, la fecha de emisión y las calificaciones.
- **Hash del Bloque Anterior:** Una huella digital criptográfica del bloque que lo precede en la cadena. Este es el elemento clave que garantiza la secuencia y la inmutabilidad de la cadena, ya que si se alterara un bloque, su hash cambiaría, invalidando la conexión con el siguiente.
- **Timestamp (Marca de Tiempo):** Un sello de tiempo que indica cuándo se creó el bloque, proporcionando un registro cronológico de los eventos.
- **Nonce y otros metadatos:** Información adicional utilizada para los mecanismos de consenso, como el que se emplea en las blockchains de prueba de trabajo (Proof-of-Work).

La interconexión de estos elementos mediante el hash crea una estructura encadenada que es virtualmente imposible de manipular sin que la red lo detecte.

¿Qué es una cadena de bloques?

La cadena de bloques, o blockchain, es una tecnología que ha trascendido su origen en las criptomonedas para convertirse en un pilar de la gestión de datos en diversas industrias. En esencia, se trata de una base de datos distribuida o un libro de contabilidad compartido entre una red de ordenadores, o nodos. A diferencia de las bases de datos tradicionales, que se almacenan en un servidor central, la blockchain replica y sincroniza la información en cada nodo de la red, lo que la hace altamente resistente a la manipulación.

Este diseño descentralizado es lo que le ha permitido desempeñar un papel crucial en los sistemas de criptomonedas, ofreciendo un registro seguro e inalterable de todas

las transacciones. Sin embargo, su potencial va mucho más allá de las finanzas, abarcando cualquier campo en el que la confianza y la seguridad de los datos sean críticas.

La característica más sobresaliente de la blockchain es su inmutabilidad. Esto significa que una vez que un bloque de datos ha sido validado y añadido a la cadena, es prácticamente imposible alterarlo o eliminarlo. La inmutabilidad se logra a través de un sofisticado sistema criptográfico que encadena cada bloque al anterior mediante una huella digital única, o hash.

Si un atacante intentara modificar un bloque, su hash cambiaría, lo que rompería la cadena y alertaría a todos los demás nodos de la red. Esta propiedad fundamental traslada la confianza del sistema a un nivel técnico: la única confianza necesaria es en el punto de entrada de los datos, ya sea un usuario o un programa. Esto elimina la dependencia de terceros confiables como auditores o intermediarios humanos, que son costosos y propensos a errores.

La aparición de Bitcoin en 2009 marcó el inicio de la revolución de la blockchain, pero desde entonces, la tecnología ha evolucionado de manera exponencial. La comunidad global de desarrolladores ha explorado y explotado sus capacidades de formas innovadoras. Han surgido miles de criptomonedas que ofrecen diferentes funcionalidades, así como aplicaciones de finanzas descentralizadas que permiten a los usuarios realizar operaciones financieras sin intermediarios.

La creación de los tokens no fungibles (NFTs) ha revolucionado la propiedad de activos digitales, y los contratos inteligentes han abierto la puerta a la automatización de acuerdos, transformando la forma en que interactuamos con el software y entre nosotros.

En la actualidad, la blockchain se utiliza para resolver desafíos en sectores tan variados como la cadena de suministro, el sector sanitario y, de manera muy relevante, la educación. En este último campo, la tecnología se aplica para la gestión de credenciales académicas, creando un sistema de certificación digital a prueba de fraudes.

Los diplomas y títulos se convierten en registros inmutables, que no pueden ser alterados, lo que protege la integridad de los logros académicos y la reputación de las instituciones. Este sistema no solo reduce la carga administrativa, sino que también empodera a los estudiantes al darles el control total sobre sus credenciales, que pueden ser verificadas de forma instantánea y segura en cualquier lugar del mundo.

1.3. Hash (Firmas criptográficas)

La función hash es el pilar de la seguridad en la blockchain. Un hash es el resultado de aplicar un algoritmo matemático a un conjunto de datos, produciendo una cadena de caracteres de longitud fija. Sus características más importantes son la unicidad, el determinismo y la irreversibilidad. En la blockchain, el hash se utiliza para identificar cada bloque de forma única y asegurar la integridad de los datos (Bit2Me Academy, 2023).

El hash del bloque anterior es la pieza que une los bloques, creando una cadena de datos interconectados.

De forma muy sencilla, podemos decir que el código hash es una sucesión alfanumérica (letras y números) de longitud fija, que identifica o representa a un conjunto de datos determinados (por ejemplo, un documento, una foto, un vídeo, etc.).

La generación de estos códigos alfanuméricos se realiza a través de lo que se llama función hash. Se trata, simplemente, de un algoritmo matemático que transforma el conjunto de datos de entrada en una expresión alfanumérica que tiene una longitud predeterminada (el código hash propiamente dicho).

Es importante destacar las siguientes características fundamentales de las funciones y códigos hash:

- Los códigos hash identifican de manera inequívoca el documento o conjunto de datos que representan. Por tanto, nunca se van a generar dos hash idénticos si los datos de entrada son diferentes o si se produce alguna alteración del input.

- Por tanto, los códigos hash son únicos. Así, si aplicamos el algoritmo sobre un mismo archivo en varias ocasiones, siempre vamos a obtener la misma secuencia alfanumérica. Por el contrario, cualquier mínima variación de los datos de entrada generarían un código hash completamente distinto.

- Las funciones hash son unidireccionales. Es decir, a partir de los datos de entrada, van a generar el código hash. Sin embargo, partiendo del código hash, no se puede descifrar o inferir cuáles fueron los datos introducidos inicialmente. Esto es fundamental para garantizar la seguridad de la tecnología.

1.4. Descentralización

La descentralización es la transferencia del control y la toma de decisiones de una entidad centralizada a una red distribuida (AWS, s.f.). En un sistema centralizado, como el de una universidad tradicional, una única entidad controla y almacena todos los registros de certificados. Esto crea un "punto único de falla" y genera dependencia. Los sistemas descentralizados, por el contrario, distribuyen la información y el poder de decisión entre todos los participantes de la red.

La blockchain, al ser un libro de contabilidad distribuido, permite que cada nodo tenga una copia del registro completo y actualizado. Esto no solo aumenta la resiliencia del sistema, sino que también fomenta la confianza, ya que no se necesita confiar en una única autoridad para validar los datos.

La **descentralización** es un modelo en el que el control y la toma de decisiones no dependen de una única entidad central, sino que se distribuyen entre múltiples participantes o nodos independientes. A diferencia de un sistema **centralizado** (como un banco o una universidad, donde una autoridad controla toda la información), en uno descentralizado (como blockchain) los datos se validan colectivamente, eliminando puntos únicos de fallo y reduciendo la necesidad de confiar en intermediarios.

La descentralización ofrece **mayor seguridad** (al evitar que un solo actor manipule el sistema), **transparencia** (todos los participantes pueden verificar los datos), **resistencia a la censura** (ninguna entidad puede bloquear transacciones) **y reducción de costos** (al eliminar intermediarios), lo que la hace ideal para aplicaciones como criptomonedas, certificados académicos y contratos inteligentes.

Figura 2: Cuadro comparativo entre centralización, distribución y descentralización.

	Centralizada	Distribuida	Descentralizada
Recursos de red/hardware	Mantenidos y controlados por una sola entidad en una ubicación centralizada	Distribuidos en varios centros de datos y geografías; propiedad del proveedor de red	Los miembros de la red poseen y comparten los recursos; son difíciles de mantener ya que nadie es propietario de ellos
Componentes de la solución	Mantenidos y controlados por una entidad central	Mantenidos y controlados por el proveedor de soluciones	Cada miembro tiene exactamente la misma copia del libro mayor distribuido
Datos	Mantenidos y controlados por una entidad central	Por lo general, son propiedad del cliente y él los administra	Solo se agregan mediante consenso grupal
Control	Controlado por la entidad central	Por lo general, una responsabilidad compartida entre el proveedor de red, el proveedor de soluciones y el cliente	Nadie es propietario de los datos y todos son propietarios de los datos

Nota. (AWS, ¿Qué es la descentralización en la cadena de bloques?, s.f.)

1.5. Inmutabilidad

La **inmutabilidad** es una de las propiedades fundamentales de la tecnología blockchain y se refiere a la incapacidad de modificar o eliminar cualquier dato una vez que ha sido registrado y validado en la cadena de bloques. Esta característica se logra mediante dos pilares tecnológicos:

1. **Estructura de Bloques Encadenados**: Cada bloque contiene un hash criptográfico único que lo vincula al bloque anterior, creando una cadena cronológica e interdependiente.
2. **Funciones Hash Criptográficas**: Algoritmos matemáticos (como SHA-256) que generan identificadores únicos e irreversibles para cada conjunto de datos.

Mecanismo de protección contra alteraciones

Si un actor malintencionado intentara manipular un certificado académico ya registrado, ocurriría lo siguiente:

- El **hash del bloque modificado cambiaría abruptamente,** rompiendo su relación con el bloque siguiente.
- Los **nodos de la red** (que almacenan copias idénticas del ledger distribuido) detectarían esta inconsistencia durante el proceso de consenso.
- La alteración sería **automáticamente rechazada**, ya que la mayoría de los nodos validarían la versión original del registro (Bitstamp, 2024).

Implicaciones para la integridad académica

Esta propiedad convierte a la blockchain en una solución óptima para prevenir el fraude en documentos educativos porque:

- **Elimina la posibilidad de falsificación**: Un título o certificado registrado en blockchain no puede ser alterado retroactivamente, ni siquiera por la institución emisora.
- **Garantiza verificación instantánea**: Cualquier entidad (empleadores, universidades) puede comprobar la autenticidad del documento sin depender de intermediarios.
- **Reduce costos administrativos**: La necesidad de procesos manuales de validación (como sellos notariales o contactos con instituciones) desaparece (Chen et al., 2021).

1.6. Contrato Inteligente (Smart Contract)

Los contratos inteligentes son la pieza clave para la automatización dentro del ecosistema blockchain, actuando como programas informáticos que se ejecutan de manera autónoma, transparente y segura una vez que se cumplen condiciones específicas. Estos programas, que residen de forma permanente en la cadena de bloques, eliminan la dependencia de intermediarios como notarios, abogados o administradores universitarios, ya que el propio código garantiza el cumplimiento de los términos de un acuerdo. Como señala IBM (2022), estos contratos "autoejecutables" permiten a los participantes confiar en la lógica del código en lugar de en una autoridad central.

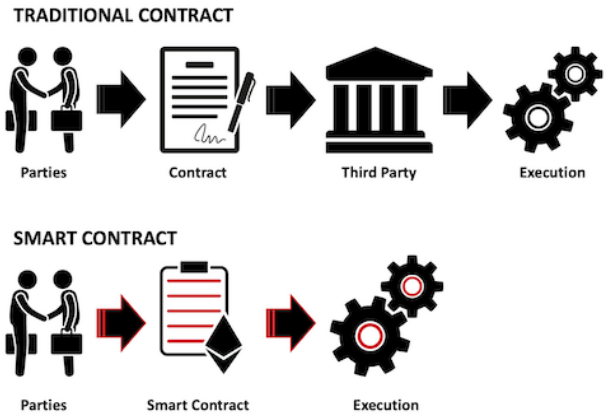
En el contexto específico de la emisión de credenciales académicas, la utilidad de los contratos inteligentes es fundamental. Un contrato inteligente podría ser programado para monitorear una base de datos descentralizada de registros de estudiantes.

Cuando este contrato detecta que un estudiante ha cumplido con todos los requisitos necesarios para un título —por ejemplo, completó un número específico de créditos, aprobó una tesis y liquidó todas sus cuotas—, se activa automáticamente.

Una vez activado, el contrato podría generar y anclar el hash del certificado digital a la blockchain, firmándolo de manera criptográfica con la clave de la universidad. Este proceso automatizado no solo agiliza el flujo de trabajo de la emisión de certificados, que tradicionalmente es manual y lento, sino que también minimiza drásticamente el riesgo de errores humanos, previene la manipulación de datos y reduce los costos administrativos asociados con la impresión, el sellado y el manejo de documentos físicos.

En esencia, el contrato inteligente asegura que la emisión de cada certificado sea un proceso infalible y eficiente, alineado con las reglas preestablecidas de la institución.

Figura 3: Comparativa entre contratos tradicionales vs contratos inteligentes.



Nota*:* https://www.1kosmos.com/article/smart-contracts/

1.7. Tecnología de Ledger Distribuido (DLT)

La Tecnología de Libro Mayor Distribuido (DLT, por sus siglas en inglés) es el concepto general del cual la blockchain es la aplicación más conocida. En su esencia, una DLT es una base de datos descentralizada y geográficamente dispersa.

A diferencia de una base de datos centralizada, que reside en un solo servidor y está controlada por una única entidad, una DLT se comparte, replica y sincroniza entre todos los nodos o participantes de la red. Esto elimina la necesidad de una autoridad centralizada para verificar y validar las transacciones. Según la Asociación Española de Banca (AEBanca, s.f.), este sistema permite que "todos los participantes tienen una copia idéntica y actualizada de la información".

Si bien la blockchain es el ejemplo más famoso de DLT —utilizada en proyectos como Bitcoin o Ethereum—, existen otras variantes que no necesariamente utilizan la estructura de bloques encadenados, como los grafos acíclicos dirigidos (DAG). Sin embargo, para la gestión de certificados académicos, la blockchain destaca como la DLT más apropiada.

Su estructura, basada en bloques de información enlazados de manera criptográfica, proporciona el alto grado de seguridad, inmutabilidad y consenso que son cruciales para un sistema de certificación. Estas características son indispensables para garantizar que cada certificado, una vez emitido, no pueda ser alterado y que su autenticidad sea verificable por cualquier participante de la red sin necesidad de recurrir a la universidad.

En otras palabras, la DLT (Tecnología de Ledger Distribuido) sienta las bases de un sistema de registro compartido, mientras que la blockchain añade las capas de seguridad y confianza necesarias para hacer de la certificación académica un proceso robusto y a prueba de manipulaciones.

2. Aplicación en el Ámbito Educativo

2.1 Credenciales físicos

Los certificados físicos universitarios son documentos impresos que validan los logros académicos de un estudiante, como la obtención de un título, un diploma o un grado. Tradicionalmente elaborados en papel de alta calidad o pergamino, estos documentos incluyen información crucial como el nombre del estudiante, el título o grado conferido, la especialidad, la fecha de graduación y el nombre de la institución. Para garantizar su autenticidad y seguridad, suelen contar con elementos de seguridad físicos, como sellos en relieve, firmas de autoridades académicas (rectores o decanos) y marcas de agua, que buscan dificultar su falsificación.

El proceso de emisión y verificación de estos certificados es, por naturaleza, manual y centralizado. Después de que un estudiante cumple con todos los requisitos académicos, la universidad prepara el documento, lo firma y lo sella. Para que un tercero, como un empleador o una institución de posgrado, verifique la autenticidad del certificado, debe contactar a la universidad emisora, lo que puede ser un proceso lento y burocrático. Esta dependencia de la institución para la validación hace que la verificación sea un cuello de botella, generando demoras y costos administrativos para todas las partes involucradas.

A pesar de su valor simbólico y su arraigo en la tradición académica, los certificados físicos presentan desafíos significativos. Su vulnerabilidad a la pérdida, el deterioro o la falsificación es considerable. Además, su naturaleza no digital limita su portabilidad y accesibilidad, ya que el estudiante debe manejar el documento físico para cualquier trámite. Estos problemas subrayan la necesidad de soluciones más modernas y seguras que puedan preservar la integridad de los logros académicos en un mundo cada vez más digital.

2.2. Credenciales Digitales

Las credenciales digitales representan una evolución significativa de los certificados tradicionales, ofreciendo una forma de reconocimiento en línea, verificable y estandarizada de las habilidades, conocimientos y logros de un individuo.

A diferencia de un simple certificado impreso o un archivo PDF estático, que son vulnerables a la falsificación y carecen de información contextual, una credencial digital basada en blockchain es un paquete de datos completo y seguro. Esta credencial no solo valida el logro, sino que también incluye metadatos detallados que proporcionan un contexto enriquecido (AcademiaBID, s.f.).

Por ejemplo, especifica la entidad que la emitió (la universidad), la persona a la que se le otorgó, los criterios exactos que se cumplieron para su obtención (como el plan de estudios o las calificaciones) y la fecha de emisión. Estas credenciales son intrínsecamente portátiles y seguras. Al estar ancladas en la blockchain, el titular no necesita depender de la institución para almacenarlas o compartirlas.

El estudiante se convierte en el dueño de su propio registro académico, lo que le otorga un control total sobre sus certificaciones. Puede compartir su credencial de manera selectiva y segura con empleadores, instituciones de posgrado o cualquier otra persona que necesite verificar su logro, sin necesidad de intermediarios.

Esta autonomía no solo simplifica el proceso de verificación, sino que también empodera al estudiante, permitiéndole construir y gestionar su trayectoria profesional y académica con una herramienta digital confiable y transparente.

2.3. Verificación de Credenciales, del proceso manual a la automatización.

La verificación de credenciales es un proceso crítico en la cadena de valor educativa y profesional, sin embargo, el modelo tradicional es ineficiente y vulnerable. Históricamente, la confirmación de un título o certificado ha dependido de una comunicación directa entre el tercero interesado (un empleador, por ejemplo) y la institución educativa. Este procedimiento manual no solo es lento y costoso, sino que también está plagado de ineficiencias administrativas y propenso a errores humanos.

La dependencia de intermediarios ralentiza los procesos de contratación, posgrado o validación, creando fricciones significativas y generando desconfianza en un sistema que debería ser incuestionable. La vulnerabilidad inherente a los certificados físicos y a los archivos digitales no seguros abre la puerta a la falsificación y manipulación, comprometiendo la integridad de los logros académicos.

Aquí es donde la tecnología blockchain ofrece una solución transformadora. Al utilizar un registro inmutable, la blockchain elimina la necesidad de intermediarios en el proceso de verificación. En lugar de enviar una solicitud formal a la universidad y esperar una respuesta, la autenticidad de un certificado se puede verificar de forma instantánea.

La universidad emite el certificado digitalmente y registra un hash único de este documento en la blockchain. Este hash funciona como una huella digital criptográfica inalterable.

Cualquier persona con acceso a este hash y al certificado digital puede utilizar una herramienta de verificación para cotejar la huella digital del documento con la que está registrada en la cadena de bloques. Si coinciden, la autenticidad del documento queda demostrada al instante.

Este nuevo modelo de verificación trae consigo beneficios significativos tanto para la universidad como para los usuarios. Para la institución, se traduce en una drástica reducción de la carga administrativa, eliminando las tediosas tareas de responder a solicitudes de validación de exalumnos.

Para los estudiantes, sus credenciales se convierten en activos digitales seguros y portátiles que pueden compartir fácilmente con la certeza de que su validez será reconocida de inmediato. Y para los empleadores, el proceso de verificación se simplifica, acortando los tiempos de contratación y brindándoles la total confianza de que están evaluando logros académicos genuinos.

En definitiva, la blockchain no solo agiliza el proceso de verificación, sino que lo redefine por completo. Como menciona ANCYPEL (2024), se elimina por completo la posibilidad de que se acepten documentos falsificados, ya que cualquier intento de manipulación rompería la conexión entre el documento y su hash registrado.

La adopción de este sistema no es solo una mejora de eficiencia, sino una medida crucial para blindar la integridad académica y restaurar la confianza en el valor de las credenciales educativas en el entorno digital.

2.4. Integridad de Datos Académicos

La integridad de los datos académicos es la piedra angular de cualquier sistema educativo, ya que su propósito es asegurar que la información contenida en los registros, como calificaciones y diplomas, sea exacta, confiable y consistente. Sin embargo, los sistemas tradicionales de gestión de registros son inherentemente vulnerables a la manipulación.

La fragilidad de los certificados impresos y la facilidad con la que se pueden alterar las bases de datos centralizadas abren la puerta a una variedad de fraudes, desde la modificación de notas hasta la creación de diplomas falsos, lo cual socava la confianza en las credenciales académicas.

La tecnología blockchain emerge como una solución robusta a este problema gracias a su característica principal: la inmutabilidad. A diferencia de una base de datos convencional, que puede ser editada o borrada, un registro en la cadena de bloques es permanente. Una vez que la universidad emite un certificado y su huella digital criptográfica (hash) se ancla en la blockchain, este registro no puede ser alterado.

Cualquier intento de modificar la información en el certificado invalidaría su hash, rompiendo la conexión con la blockchain y haciendo evidente la manipulación. Esto crea una barrera impenetrable contra el fraude y asegura que el historial académico de un estudiante sea un reflejo veraz y permanente de sus logros.

Esta inmutabilidad no solo previene la falsificación, sino que también establece una capa de seguridad y confianza sin precedentes. La Fundación Aula Smart (2018) lo resume perfectamente, señalando que la blockchain ofrece un "marco sólido para garantizar la seguridad y la integridad de los datos educativos". Al dotar a los registros de una validez incuestionable, se protege la reputación de la universidad, se valida el esfuerzo de los estudiantes y se refuerza la confianza de los empleadores y la sociedad en las credenciales académicas. En esencia, la blockchain convierte la integridad de los datos de un ideal a una certeza técnica, resolviendo desafíos de seguridad que los sistemas tradicionales simplemente no pueden abordar de manera efectiva.

2.5. Identidad Digital Soberana (SSI)

La Identidad Digital Soberana (SSI) es un concepto revolucionario que cambia el paradigma de la gestión de datos personales. Tradicionalmente, nuestra información digital, incluidos nuestros logros académicos, está fragmentada y controlada por terceros: las universidades tienen nuestros diplomas, los bancos nuestra información financiera y los hospitales nuestros registros médicos.

Este modelo centralizado nos deja vulnerables y sin control sobre nuestros propios datos. La SSI propone una solución a esta dependencia al empoderar a los individuos, dándoles la capacidad de ser los custodios de su propia identidad y de sus registros, sin necesidad de que una autoridad central actúe como intermediario.

La tecnología blockchain se convierte en el habilitador técnico de la SSI, ofreciendo un medio seguro e inmutable para almacenar y gestionar credenciales verificables. En el contexto educativo, esto se manifiesta cuando un estudiante recibe un certificado digital basado en blockchain. En lugar de que la universidad controle el acceso a este documento, el estudiante lo almacena de forma segura en su cartera digital. Como explica

Amo Filvà (2020), este sistema fomenta la autonomía y la privacidad, ya que el estudiante es quien decide selectivamente qué información compartir, cuándo y con quién, sin necesidad de pedir permiso a la institución emisora.

Esta capacidad de gestionar su propio historial académico transforma por completo la relación entre el estudiante y sus logros. Un estudiante puede, por ejemplo, compartir una credencial específica de un curso con un potencial empleador, mientras retiene otra información más sensible. Este control granular no solo protege la privacidad del individuo, sino que también agiliza los procesos de verificación, ya que el estudiante puede presentar sus credenciales de manera directa y segura. La SSI, por tanto, no es solo una mejora técnica, sino un paso fundamental hacia un futuro en el que las personas son dueñas de su identidad y sus datos, lo cual representa un avance significativo en la confianza y la seguridad del ecosistema educativo.

2.6. Certificado Basado en Blockchain

El certificado basado en blockchain es la culminación de la implementación de esta tecnología en el ámbito académico. A diferencia de los diplomas tradicionales, que son meros documentos físicos o archivos digitales estáticos, el certificado en blockchain es un activo digital seguro, verificable y con un valor intrínseco.

Sus características esenciales lo distinguen por completo de cualquier formato anterior. En primer lugar, se trata de un documento digital único, que incluye todos los datos académicos relevantes del estudiante. Lo crucial, sin embargo, es que su huella digital criptográfica, o hash, se registra en la blockchain, actuando como un ancla inalterable que prueba su existencia y validez.

Además de su inmutabilidad, este tipo de certificado se distingue por su seguridad criptográfica y su portabilidad. La universidad, al emitirlo, lo firma digitalmente con su clave privada, lo que garantiza la autenticidad de la fuente.

Esta firma puede ser verificada por cualquier persona con la clave pública de la universidad, eliminando cualquier duda sobre la legitimidad del documento. Y, más importante aún, este sistema empodera al estudiante. A diferencia de los certificados

físicos que deben ser resguardados y presentados, el certificado en blockchain es un activo que el estudiante posee y controla por completo. Puede ser almacenado de manera segura en una cartera digital y compartido selectivamente, sin tener que depender de la universidad para su verificación.

Esta combinación de características convierte a los diplomas y títulos en documentos verdaderamente infalsificables, portables y verificables en cualquier parte del mundo. Como se ha señalado, la implementación de este sistema no solo moderniza el proceso de emisión, sino que también protege el valor de la educación (Thomas Signe, s.f.).

Al garantizar la autenticidad y la integridad de las credenciales, la tecnología blockchain refuerza la confianza en el sistema educativo y prepara a los estudiantes para un futuro profesional en el que la verificación de logros sea un proceso transparente, instantáneo y a prueba de fraudes.

3. Aspectos Técnicos y de Implementación

3.1. Plataformas Blockchain para la Educación (Ethereum Solana y Otros)

Si bien el concepto de blockchain es la base de la certificación digital, la implementación práctica depende de la elección de una plataforma blockchain específica, cada una con sus propias características y fortalezas. Ethereum se ha consolidado como una de las opciones más populares para el desarrollo de soluciones de certificación académica, y su principal ventaja reside en su capacidad para ejecutar contratos inteligentes.

Estos programas autónomos permiten la automatización de procesos complejos, como la emisión automática de un certificado una vez que se cumplen los requisitos académicos, o la verificación instantánea de su validez por parte de un tercero. Gracias a su naturaleza de código abierto, Ethereum cuenta con una comunidad de desarrolladores amplia y activa, que ha creado un ecosistema robusto y lleno de herramientas para la construcción de aplicaciones descentralizadas (dApps), lo cual facilita la innovación y el desarrollo de proyectos a medida.

Sin embargo, en el panorama actual han surgido competidores que buscan mejorar aspectos clave como la velocidad y el costo de las transacciones. Solana, por ejemplo, se ha posicionado como una alternativa de alto rendimiento, famosa por su gran velocidad de procesamiento y sus comisiones de transacción (gas fees) significativamente más bajas que las de Ethereum.

Esto la convierte en una opción atractiva para instituciones que necesitan emitir y verificar un gran volumen de certificados de manera eficiente y a bajo costo. A diferencia de Ethereum, Solana utiliza un mecanismo de consenso híbrido que combina la prueba de participación (Proof-of-Stake) con la prueba de historia (Proof-of-History), lo que le permite alcanzar una escalabilidad impresionante sin sacrificar la seguridad.

Otras plataformas como Hyperledger Fabric y Cardano también se perfilan como opciones viables, cada una pensada para diferentes necesidades. Hyperledger Fabric, por ejemplo, es una plataforma de código abierto orientada a soluciones empresariales y redes privadas, lo que la hace ideal para consorcios de universidades que buscan un mayor control sobre su red de certificación.

Por su parte, Cardano se distingue por su enfoque en la seguridad y la sostenibilidad, utilizando un protocolo de consenso de prueba de participación que consume menos energía que el de Ethereum. La decisión de cuál plataforma utilizar es crucial y debe basarse en una evaluación cuidadosa de los requisitos específicos del proyecto.

La selección de la plataforma debe considerar factores como el tipo de red (pública o privada), la escalabilidad, el costo de las transacciones, la seguridad y la facilidad de desarrollo. Para una universidad que busca un sistema de certificación transparente y abierto para el público, una plataforma como Ethereum o Solana, con su naturaleza pública, podría ser la más adecuada.

Por el contrario, si el objetivo es crear una red cerrada para la verificación de certificados entre un grupo selecto de instituciones, una plataforma privada como Hyperledger Fabric podría ofrecer un mejor rendimiento y mayor control. En cualquier

caso, la elección correcta es un paso fundamental para asegurar el éxito y la sostenibilidad de la solución de certificación académica.

¿Qué es Ethereum?

Ethereum es una plataforma de blockchain descentralizada que se ha consolidado como un pilar fundamental en el mundo de las criptomonedas. Lanzada en 2015 por Vitalik Buterin, esta red se distingue de otras como Bitcoin por su capacidad para ir más allá de las simples transacciones de valor.

Su característica más revolucionaria es la funcionalidad de los contratos inteligentes, programas autónomos que se ejecutan automáticamente cuando se cumplen ciertas condiciones. Esto ha permitido a los desarrolladores crear una vasta gama de aplicaciones descentralizadas (DApps) que forman la base de ecosistemas innovadores como las finanzas descentralizadas (DeFi) y los tokens no fungibles (NFT).

El token nativo de la red, Ether (ETH), no solo se utiliza para transacciones, sino que también es el combustible para ejecutar estos contratos inteligentes y las operaciones de las DApps. Originalmente, Ethereum operaba bajo un mecanismo de consenso de prueba de trabajo (PoW), similar a Bitcoin, pero en una transformación conocida como Ethereum 2.0, migró a la prueba de participación (PoS), un modelo más escalable y eficiente en términos energéticos.

¿Qué es Solana?

Solana es una plataforma de blockchain de alto rendimiento que fue diseñada específicamente para resolver los problemas de escalabilidad que enfrentaban las redes descentralizadas, particularmente Ethereum. Lanzada en 2020, Solana utiliza una combinación de tecnologías innovadoras, siendo la más notable su algoritmo de Prueba de Historia (PoH).

Este mecanismo le permite procesar un volumen masivo de transacciones, con velocidades que pueden superar las 65,000 transacciones por segundo, a un costo

significativamente bajo para los usuarios. Esta arquitectura de alto rendimiento hace de Solana una de las blockchains más rápidas disponibles.

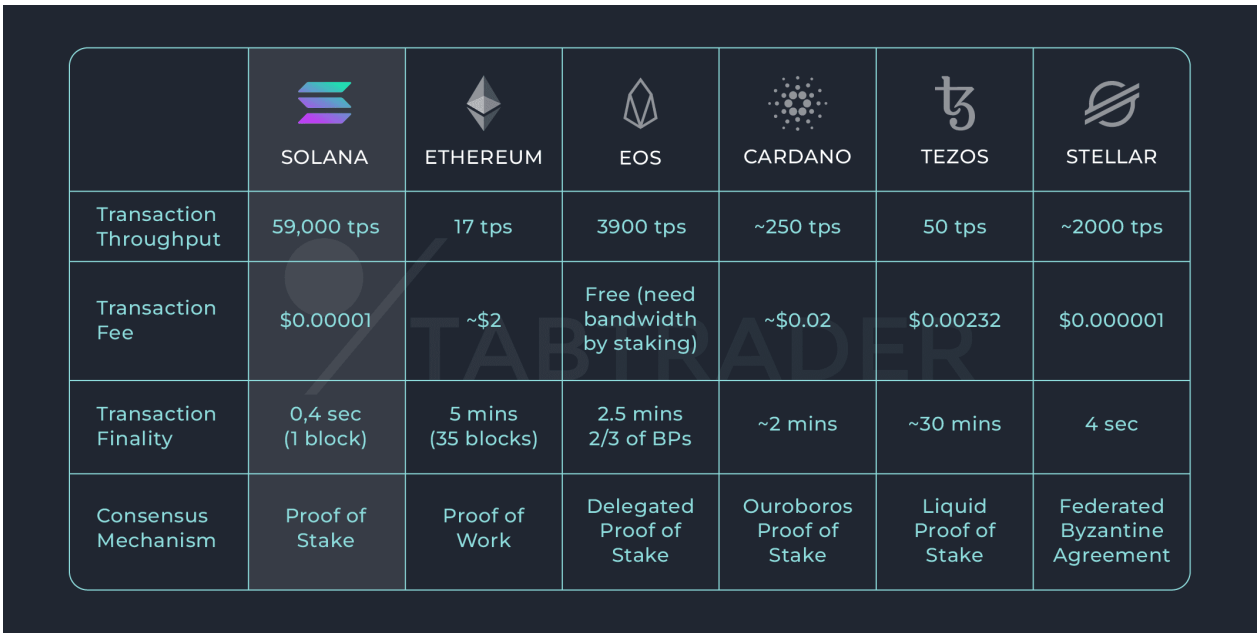
El funcionamiento de la red es impulsado por su criptomoneda nativa, Solana (SOL), que cubre los costos de las transacciones y la ejecución de los programas que equivalen a los contratos inteligentes. Sin embargo, a lo largo de su historia, la red ha enfrentado críticas y ha generado debates sobre su nivel de descentralización real, debido a incidentes que han planteado dudas sobre si un grupo reducido de entidades tiene demasiado control sobre su funcionamiento.

Comparativa entre Solana y Ethereum

Tanto Solana como Ethereum se han establecido como líderes en el desarrollo de aplicaciones descentralizadas, los NFTs y las finanzas descentralizadas. Aunque ambos comparten el objetivo de ser plataformas robustas para el desarrollo, sus arquitecturas y filosofías presentan diferencias clave.

Mientras que Ethereum, con su vasta trayectoria, se ha enfocado en la seguridad y una descentralización más probada, Solana ha priorizado la velocidad y la escalabilidad, intentando ofrecer una alternativa más rápida y económica. La elección entre ambas plataformas a menudo depende de las necesidades específicas de los desarrolladores: Ethereum podría ser preferido para aplicaciones que demandan una seguridad y estabilidad incuestionables, mientras que Solana sería ideal para proyectos que requieran un alto volumen de transacciones a bajo costo. A pesar de sus diferencias, ambas redes son cruciales en la evolución de las finanzas y la tecnología descentralizada, y los desarrolladores continúan trabajando para superar sus respectivas limitaciones.

Figura 4: Compartiva entre las diferentes tecnología de blockchain



Nota: (Solana vs Ethereum, s.f.)

3.2. Tokenización

La tokenización es un concepto fundamental en la aplicación de la blockchain, que consiste en la creación de una representación digital de un activo físico o intangible. Este proceso permite que un objeto, como una obra de arte, una propiedad o, en este caso, un certificado académico, se convierta en un activo digital que puede ser gestionado y transferido en una cadena de bloques.

En el contexto educativo, la tokenización no es solo una digitalización; es una forma de dotar a los logros académicos de un estatus de activo digital único, seguro e infalsificable.

Un ejemplo claro de tokenización en la certificación académica es el uso de los tokens no fungibles (NFT). Los NFT son tokens únicos e indivisibles que demuestran la propiedad de un activo digital específico. A diferencia de un activo fungible como una moneda, donde un token es idéntico a otro, cada NFT es único, lo cual lo hace perfecto para representar un diploma o un título. Cada certificado académico se podría convertir

en un NFT único, con una identidad digital que lo distingue de todos los demás. Este token contiene metadatos cruciales, como el nombre del estudiante, el título obtenido y la fecha de emisión, asegurando que el registro de cada logro sea insustituible y singular.

La tokenización de los certificados ofrece una prueba de propiedad y autenticidad indiscutible. Al ser un registro inmutable en la blockchain, se elimina la posibilidad de fraude, ya que el token y los metadatos asociados no pueden ser alterados. Este sistema garantiza que la credencial digital pertenezca de forma exclusiva al estudiante, quien tiene el control total sobre ella.

Como resalta Signeblock (2025), esta metodología no solo combate el fraude, sino que también empodera a los estudiantes al convertirlos en los verdaderos dueños de sus credenciales, permitiéndoles gestionar y compartir su historial académico de forma segura y autónoma.

La tokenización de certificados va más allá de la simple digitalización, al transformar los diplomas en activos digitales seguros y únicos. Al convertirlos en NFT, se dota a cada credencial de una identidad digital irrefutable, garantizando su autenticidad y propiedad. Este proceso no solo moderniza la forma en que las instituciones educativas emiten sus documentos, sino que también establece un nuevo estándar de seguridad y control para los estudiantes sobre sus logros académicos.

NFT (Tokens No Fungibles)

Los NFTs (Tokens No Fungibles) son un concepto fundamental que ha ganado gran popularidad en el ecosistema blockchain. A diferencia de las criptomonedas como Bitcoin o Ether, que son fungibles (es decir, una unidad es idéntica y se puede intercambiar por otra), un NFT es un token único e indivisible. Su valor reside precisamente en esa singularidad, ya que cada NFT representa un activo digital o físico de manera exclusiva.

Debemos pensar en ellos como certificados de autenticidad y propiedad inmutables, pero en formato digital. Esta cualidad los ha convertido en la herramienta perfecta para la tokenización, que es el proceso de convertir un activo en un token

blockchain, permitiendo su registro, transferencia y gestión de forma segura y transparente.

La tecnología detrás de los NFTs se basa en contratos inteligentes que residen en una blockchain, siendo Ethereum la plataforma pionera en su estandarización. Estos contratos inteligentes no solo definen las reglas del token, como su creación y transferencia, sino que también almacenan los metadatos que lo hacen único.

Estos metadatos pueden incluir el nombre del activo, una descripción, un enlace a un archivo (como una imagen, un video o un archivo de audio) y cualquier otra información relevante. La combinación del token y sus metadatos es lo que garantiza su unicidad y verificabilidad. Al estar en una blockchain, el registro de propiedad de un NFT es público y no puede ser alterado, lo que elimina el riesgo de falsificación o disputas sobre la autenticidad del activo.

Originalmente, los NFTs se hicieron famosos por su uso en el arte digital y los coleccionables, creando un nuevo mercado para creadores y coleccionistas. Sin embargo, su potencial va mucho más allá. La tokenización a través de NFTs se puede aplicar a una amplia variedad de activos, desde bienes inmuebles y artículos de lujo hasta la propiedad intelectual y, de manera muy relevante para tu proyecto, los certificados académicos.

En este contexto, un diploma o un título universitario se puede tokenizar, convirtiéndose en un NFT que representa de manera única los logros de un estudiante. Este NFT contendría todos los datos del certificado, asegurando su autenticidad e inmutabilidad.

La emisión de certificados como NFTs ofrece una solución definitiva a los problemas de fraude y verificación. Una vez que la universidad emite el certificado como un NFT, este se convierte en un activo digital que el estudiante posee y controla.

La titularidad del NFT es pública y verificable en la blockchain, por lo que cualquier empleador o institución puede comprobar la autenticidad del diploma de forma

instantánea y sin necesidad de contactar a la universidad. Este proceso empodera al estudiante, dándole el control total de sus credenciales, mientras que a las instituciones les brinda una herramienta para proteger su reputación y la integridad de sus títulos de una manera que los certificados físicos no pueden.

En resumen, los NFTs son mucho más que activos digitales para el arte. Son una tecnología de confianza que permite la creación de activos únicos, seguros y verificables en un entorno digital. Su aplicación en la certificación académica representa un avance significativo, ya que no solo moderniza un proceso tradicional, sino que también establece un nuevo estándar de seguridad y control, beneficiando a estudiantes, instituciones y empleadores por igual.

Figura 5: Representación de uno de los NFT más famosos y populares, uno de estos llegó a costar más de un millón de dólares.

Nota: (Computer, s.f.)

3.3. Seguridad Criptográfica

La seguridad inherente de la tecnología blockchain, que la hace tan confiable para la emisión de certificados, se basa en un pilar fundamental: la criptografía. Esta disciplina matemática no solo protege las transacciones y los datos, sino que también garantiza la autenticidad de los participantes en la red.

En el corazón de este sistema se encuentra la criptografía de clave pública y privada, un método robusto que crea una conexión irrompible entre un emisor y un receptor. A través de este sistema, cada usuario o entidad en la red, ya sea una universidad o un estudiante, tiene un par de claves únicas: una clave privada que se mantiene en secreto y una clave pública que se puede compartir libremente.

El sistema de clave pública y privada es la base de la autenticación y la integridad de los datos. La clave privada, como su nombre lo indica, es un secreto personal que se usa para firmar digitalmente cualquier documento o transacción que el usuario quiera autenticar. Esta firma es una prueba criptográfica de que el usuario es el verdadero dueño de la clave privada y que aprobó la acción.

Por otro lado, la clave pública es una herramienta de verificación que permite a cualquier persona comprobar si una firma digital es legítima, sin necesidad de conocer la clave privada. Este mecanismo de seguridad asimétrica es lo que permite que las interacciones en la blockchain se realicen sin la necesidad de confiar en un intermediario.

En el contexto de la certificación académica, este sistema criptográfico es fundamental para asegurar la validez de los diplomas. Cuando la universidad emite un certificado digital, utiliza su clave privada para firmarlo. Esta firma digital se convierte en una huella criptográfica que demuestra, de forma irrefutable, que el documento proviene de la entidad legítima. Esta firma se ancla al certificado y, a su vez, a la blockchain.

Cualquier persona que reciba este certificado, como un empleador o una institución de posgrado, puede usar la clave pública de la universidad para verificar la firma digital. Si la firma es auténtica, la persona tiene la certeza de que el certificado fue emitido por la universidad.

Además de verificar la autenticidad, la criptografía garantiza la inmutabilidad del certificado. La firma digital está intrínsecamente vinculada al contenido del documento. Esto significa que si alguien intentara alterar la información del certificado, aunque fuera un solo carácter, la firma digital dejaría de ser válida.

La verificación con la clave pública de la universidad fallaría de inmediato, alertando a cualquiera que intente validar el documento de que ha sido manipulado. Esto crea una capa de seguridad y confianza que es casi imposible de replicar en un sistema de certificación tradicional.

En resumen, la seguridad criptográfica no es solo una función adicional de la blockchain, sino su componente central. La combinación del sistema de clave pública y privada con la naturaleza inmutable de la cadena de bloques asegura que los certificados académicos sean auténticos, verificables y resistentes a cualquier forma de manipulación. Esto convierte a los diplomas en documentos digitales fiables, que benefician tanto a las instituciones que los emiten como a los estudiantes y a los empleadores que los utilizan.

¿Qué es la criptografía?

La criptografía es la ciencia de proteger información mediante técnicas matemáticas, convirtiendo datos legibles (*texto plano*) en formatos ilegibles (*texto cifrado*) que solo pueden descifrarse con una clave específica. Su objetivo es garantizar **confidencialidad, integridad y autenticidad** en las comunicaciones digitales (AWS, 2024).

Funciones Clave de la Criptografía

1. **Cifrado (Encriptación):**
    - **Cifrado simétrico**: Usa la misma clave para cifrar y descifrar (ej.: AES).
    - **Cifrado asimétrico**: Emplea un par de claves (pública y privada), como RSA o ECC.
2. **Funciones Hash:**

- Algoritmos (ej.: SHA-256) que generan un *hash* único e irreversible a partir de datos. Usados en blockchain para garantizar inmutabilidad.

3. **Firmas Digitales:**
    - Permiten verificar la autenticidad de un mensaje o documento mediante criptografía asimétrica (AWS, 2024).

CAPITULO III. MARCO METODOLÓGICO

3.1 Tipo de investigación

3.1.1 Finalidad

Definiciones de Conceptos Metodológicos

1. Tipo de Investigación según su Finalidad

La finalidad de una investigación se refiere al propósito principal que persigue el estudio. Según la literatura, se pueden clasificar en teórica o aplicada.

- **Investigación Teórica:** Este tipo de investigación tiene como objetivo generar nuevo conocimiento, ampliar o contrastar teorías existentes, sin que necesariamente se busque una aplicación práctica o una solución inmediata a un problema específico. Su finalidad es puramente académica, contribuyendo al avance del conocimiento científico (Hernández-Sampieri, Fernández-Collado & Baptista-Lucio, 2014).
- **Investigación Aplicada:** A diferencia de la teórica, la investigación aplicada se enfoca en resolver problemas prácticos o mejorar situaciones concretas. Utiliza el conocimiento generado por la investigación teórica para aplicarlo en contextos específicos, con el fin de generar un resultado tangible que pueda ser implementado (Díaz-Barriga Arceo & Hernández Rojas, 2002).

2. Tipo de Investigación según su Enfoque Sistemático

El enfoque sistemático se refiere al nivel de complejidad o al alcance geográfico y social del estudio. Si bien no existe una clasificación única y universalmente aceptada, se puede entender la siguiente diferenciación:

- **Enfoque Macro:** Implica el estudio de fenómenos a gran escala, como el impacto de una política educativa a nivel nacional o global. Se centra en la interconexión de sistemas complejos.
- **Enfoque Meso:** Se sitúa en un nivel intermedio, centrándose en el análisis de organizaciones, instituciones o sectores específicos. Es común en estudios que

buscan comprender la dinámica de una empresa, una universidad o una comunidad particular (Montero & León, 2007).

- **Enfoque Micro:** Se enfoca en el análisis de fenómenos a pequeña escala, como el comportamiento de individuos, grupos reducidos o procesos muy específicos dentro de una organización.

3. Tipo de Investigación según su Naturaleza

La naturaleza de la investigación se refiere al tipo de datos que se recolectan y analizan.

- **Investigación Cuantitativa:** Este enfoque utiliza la recolección y el análisis de datos numéricos para probar hipótesis o establecer patrones de comportamiento. Su objetivo es medir, cuantificar y generalizar los resultados a partir de una muestra a una población (Hernández-Sampieri et al., 2014).
- **Investigación Cualitativa:** La investigación cualitativa se centra en la comprensión de fenómenos a través de la recolección de datos no numéricos, como narrativas, percepciones, experiencias y observaciones. Su propósito es interpretar la realidad social y las motivaciones de los participantes (Valles, 2000).

4. Tipo de Investigación según su Carácter

El carácter de una investigación se relaciona con el propósito y el tipo de preguntas que el estudio busca responder.

- **Investigación Descriptiva:** Busca caracterizar, describir o identificar las propiedades de un fenómeno o de una población. Su objetivo no es explicar por qué algo ocurre, sino simplemente describir cómo es (Hernández-Sampieri et al., 2014).
- **Investigación Explicativa:** Tiene como objetivo encontrar las causas de un fenómeno. Responde a la pregunta "¿por qué?" y busca establecer relaciones entre variables para explicar su comportamiento (Kerlinger & Lee, 2002).

- **Investigación Causal:** Similar a la explicativa, pero se enfoca en establecer una relación directa de causa y efecto entre variables. Se utiliza en estudios experimentales para determinar el impacto de una variable sobre otra.
- **Investigación Comprensiva:** Busca interpretar y comprender un fenómeno en su contexto, desde la perspectiva de los actores involucrados. Se enfoca en el "significado" que los participantes le dan a sus experiencias (Stake, 1995).

Tipo de investigación y metodología elegidas

El presente proyecto se fundamenta en un marco metodológico riguroso, diseñado para guiar la investigación y el diseño de una solución de certificación académica basada en tecnología blockchain. A continuación, se detallan los elementos que definen el abordaje de este trabajo.

Tipo de Investigación

Esta investigación se define por su finalidad aplicada, ya que su propósito no es solo generar conocimiento teórico, sino también proponer una solución concreta a una problemática real en la Universidad Internacional San Isidro Labrador. El enfoque planteado es meso, centrado en el estudio y la planificación de una solución para una institución específica, en este caso, la Universidad Internacional San Isidro Labrador, Sede Central.

La naturaleza de esta investigación es cualitativa, ya que se enfoca en la comprensión de percepciones y opiniones de los actores clave, en lugar de en la recolección de datos numéricos. Esto permitirá obtener una visión profunda de los procesos y las necesidades de los involucrados.

El carácter de esta investigación es descriptivo, explicativo, causal y comprensivo. Es descriptivo porque se detallarán los procesos actuales de emisión de certificados y las funcionalidades de la tecnología blockchain. Es explicativo porque se analizará por qué la tecnología blockchain es una solución superior a los métodos actuales.

Es causal en la medida en que se establecerá una relación entre la implementación de blockchain y la potencial reducción del fraude. Finalmente, es comprensivo porque se buscará entender las implicaciones y el impacto de la solución propuesta desde la perspectiva de los diferentes actores.

3.2 Administración y abordaje del proyecto objeto

3.2.1 Descripción de supuestos

La viabilidad del proyecto se sustenta en dos premisas fundamentales. Primero, se asume que la tecnología blockchain es un método efectivo para prevenir el fraude en certificados académicos. Segundo, se parte de la premisa de que la universidad está dispuesta a considerar una solución de este tipo, y que su implementación traerá mejoras significativas en la eficiencia administrativa.

3.2.2 Restricciones y riesgos

Entre las principales restricciones y riesgos identificados, se encuentra el presupuesto, ya que la implementación de plataformas como Ethereum puede implicar costos considerables. Además, el proyecto está limitado a la etapa de definición y planificación, por lo que no se llevará a cabo una implementación real ni una evaluación de resultados.

3.3 Sujetos y fuentes de información

3.3.1 Sujetos de Información

Los sujetos de estudio del presente proyecto de investigación fueron los colaboradores de los diferentes departamentos involucrados en la elaboración de certificados académicos, así como un pequeño muestreo de empleadores de los egresados de la Universidad Internacional San Isidro Labrador, los cuales fueron fuente para recolección de información con el propósito de responder a las interrogantes de investigación relacionadas con las variables de investigación.

A continuación, se muestra la lista de sujetos con su respectivo cargo/empresa:

Tabla 1: Sujetos de investigación – Funcionarios UISIL

NOMBRE	CARGO
PhD. Carlos Cortés Sandí	Rector
Ing. David Venegas Gamboa	Gerente Administrativo
MsC. Kiara Angulo Hidalgo	Directora del Departamento de Registro
Lic. Esteban Quesada Hidalgo	Director del Centro de Especializaciónón.
MBA. Andrea Mesén Hidalgo	Coordinadora del Centro de Especialización.

Nota: Elaboración propia

Tabla 2: Sujetos de investigación – Empresas, posibles empleadores

NOMBRE	EMPRESA
Idianey Guillén	Credecoop R. L.
Wendy Díaz	CTS
Fabian Montenegro	Consulting and Training Solutions S. A.
Marielos Ugalde	Emprendedores de Pérez Zeledón
Jeison Mena	SISTEC de Costa Rica
Cristina Naranjo	Coopealianza
Orlando Piedra	SID de Costa Rica
Alejandro Mora	SID
Joseph Alvarado	Grupo J&F Consultores
Erick Cerdas	TecnoSoluciones Brunca S. A.

Nota: Elaboración propia

3.3.2 Fuentes de información

Según la obra "Metodología de la investigación" (3ra ed.) de Bernal, C. A. (2010), existen dos categorías principales para la recopilación de datos: las fuentes primarias y las secundarias. (Bernal, 2010)

Las fuentes primarias son aquellas que proporcionan información de primera mano o directa, es decir, se obtiene justo en el lugar de origen de los hechos o la

situación. Ejemplos de estas fuentes incluyen personas, organizaciones, acontecimientos y el entorno natural.

Por su parte, las fuentes secundarias son recursos que ofrecen información sobre el tema de estudio, pero no provienen directamente del origen de los hechos, sino que los referencian o los documentan. Las fuentes secundarias más comunes abarcan libros y revistas, todo tipo de material impreso o documentos escritos, documentales, noticieros y medios de comunicación.

3.4 Muestreo

3.4.1 Población y muestreo

Los sujetos de información son los individuos y grupos clave cuyas opiniones y experiencias son cruciales para el proyecto.

Para este estudio, los sujetos de información incluyen a empleados del Centro de Extensión Universitaria (CEU), personal del Departamento de Registro, Gerencia y Rectoría. Estos actores tienen una visión directa de los procesos de emisión y validación de certificados y, por lo tanto, sus perspectivas son esenciales para el diseño de una solución efectiva. Además, se contará con la opinión de una pequeña muestra de empleadores de nuestros estudiantes, los cuales son parte del proceso de validación de certificados.

Las fuentes de información son principalmente de tipo primario, ya que los datos se recolectarán directamente de los sujetos a través de instrumentos de investigación diseñados para este proyecto.

3.4.2 Tipo de muestreo

Para la recolección de información, se utilizarán dos técnicas principales. La primera es un muestreo de conveniencia de empresas del sector profesional que deseen verificar certificados. A este grupo se les aplicará una encuesta con preguntas cerradas

para conocer su percepción sobre los sistemas de verificación actuales y la posible utilidad de una plataforma basada en blockchain.

La segunda técnica consistirá en entrevistas a profundidad con los sujetos de información dentro de la universidad. Estas entrevistas permitirán obtener una comprensión detallada de los procesos actuales, los puntos débiles y las expectativas con respecto a la nueva solución.

3.5 Diseño de técnicas e instrumentos para recolectar información

3.5.1 Detalle de técnica e instrumentos de aplicación

Se utilizarán dos técnicas principales para la recolección de datos, cada una con su instrumento específico: la encuesta para las empresas del sector profesional y la entrevista para los actores clave dentro de la universidad.

1. Técnica: Encuesta

- **Instrumento: Cuestionario estructurado (o de preguntas cerradas)**.
    - **Objetivo:** Recolectar datos **cuantitativos** sobre la percepción y experiencia de las empresas externas con respecto a la verificación de certificados y la viabilidad/utilidad de una solución basada en *blockchain*.
    - **Población de aplicación:** Empresas del sector profesional (10 empresas)
    - **Contenido:**
        - Frecuencia con la que verifican certificados.
        - Problemas o demoras experimentadas en el proceso de verificación actual.
        - Nivel de interés en utilizar una plataforma de verificación instantánea y segura basada en *blockchain*.
        - Valoración de atributos como confiabilidad, rapidez y seguridad en la verificación.

2. Técnica: Entrevista

- **Instrumento: Guía de entrevista semi-estructurada (o a profundidad)**.
    - **Objetivo:** Obtener información cualitativa y detallada sobre los procesos internos de emisión y validación de certificados, identificar problemas (cuellos de botella, riesgos, costos) y conocer las expectativas y requisitos funcionales y no funcionales para la nueva solución.
    - **Población de aplicación:** Sujetos de información clave (Empleados del CEU, Personal de Registro, Gerencia y Rectoría).
    - **Contenido (Ejemplos):**
        - Puesto y funciones principales relacionadas con la emisión de certificados.
        - Descripción del flujo de trabajo actual para la emisión y validación.
        - Principales desafíos o puntos débiles del proceso actual.
        - Información crucial que debe contener el certificado digital.
        - Requisitos de seguridad y acceso para el nuevo sistema.
        - Percepción sobre la implementación de tecnología *blockchain*.

3.5.2 Detalle de la aplicación de técnicas e instrumentos

La aplicación de las técnicas e instrumentos se llevará a cabo en dos fases distintas, dirigidas a las dos poblaciones objetivo.

1. Aplicación de la Encuesta (Muestreo de Conveniencia - Empresas)

- **Método de Aplicación:** Se utilizará un formulario digital en línea elaborado Google Forms para facilitar la distribución, recolección y análisis de los datos. Esto permite un alcance amplio y reduce costos.
- **Procedimiento:**
    1. **Contacto Inicial:** Identificación de empresas colaboradoras dispuestas a participar a través de contacto directo con proveedores de la Universidad y con empresas reclutadoras encontradas en la red social LinkedIn.

2. **Distribución:** Envío del enlace al cuestionario estructurado a los responsables de Recursos Humanos o Talento Humano de las empresas contactadas, ya que son los que típicamente manejan la verificación de credenciales.
3. **Recolección:** Se establecerá un plazo definido para la respuesta, con recordatorios para maximizar la tasa de participación.

- **Resultado Esperado:** Datos cuantificables sobre la necesidad y aceptación externa de la propuesta de valor basada en blockchain.

2. Aplicación de la Entrevista (Sujetos de Información - Universidad)

- **Método de Aplicación:** Entrevistas personales para asegurar un ambiente que promueva la apertura y profundidad en las respuestas. La entrevista será grabada (con consentimiento) para su posterior transcripción y análisis.
- **Procedimiento:**
    1. **Selección y Programación:** Se contactará directamente a los sujetos clave (CEU, Registro, Gerencia, Rectoría) para explicar el objetivo del estudio y agendar una hora que no interfiera con sus labores.
    2. **Ejecución:** Se aplicará la guía de entrevista semi-estructurada. El entrevistador debe asegurarse de cubrir todos los puntos clave de la guía, permitiendo al mismo tiempo que el sujeto profundice en temas relevantes no previstos inicialmente.
    3. **Análisis:** Los datos recolectados (transcripciones) se analizarán mediante codificación temática para identificar patrones, requisitos, riesgos y flujos de proceso.
- **Resultado Esperado:** Comprensión profunda del "estado actual" de los procesos, la identificación de los problemas internos y la articulación clara de los requisitos funcionales y técnicos para la solución blockchain.

3.6 Determinación de variables

3.6.1 Clasificación

El estudio está estructurado alrededor de una Variable Independiente (Causa), que es la solución propuesta, y varias Variables Dependientes (Efecto), que son los resultados o impactos esperados de dicha solución. La variable independiente central es la Plataforma de Certificación Basada en Blockchain, ya que es el elemento que se está diseñando y evaluando. Las variables dependientes principales se agrupan en torno a los ejes de eficiencia operativa y percepción externa:

Eficacia del Proceso de Emisión y Validación, medida por la reducción de tiempo y la mitigación de fallas; la Seguridad y Confianza en la Verificación de Certificados, medida por la reducción de fraude y la percepción de autenticidad; y la Aceptación y Usabilidad Tecnológica por parte de los usuarios internos y externos.

Las variables secundarias o intervinientes incluyen la Infraestructura Tecnológica Actual de la universidad y las Políticas y Regulaciones Internas sobre la gestión de documentos, las cuales pueden influir en la implementación de la plataforma.

3.6.2 Definición

La Plataforma de Certificación Basada en Blockchain se define como el sistema digital descentralizado y distribuido que utiliza la tecnología de cadena de bloques para la emisión inmutable, el registro seguro y la validación instantánea de los certificados académicos emitidos por la institución.

La Eficacia del Proceso de Emisión y Validación se define como el grado en que la nueva plataforma logra simplificar y acelerar el flujo de trabajo interno, reduciendo los tiempos de ciclo y minimizando los errores operativos asociados con la gestión manual o centralizada de certificados.

La Seguridad y Confianza en la Verificación de Certificados se define como la garantía proporcionada por el sistema blockchain de que un certificado es auténtico, inalterable y rastreable, lo que se traduce en una reducción demostrable de intentos de fraude y un aumento en la fiabilidad percibida por las empresas externas.

Finalmente, la Aceptación y Usabilidad Tecnológica se define como la disposición y facilidad con la que tanto los empleados del CEU y Registro, como las empresas verificadoras, adoptan e interactúan con la interfaz y las funcionalidades de la plataforma blockchain, evaluando su curva de aprendizaje, satisfacción y eficiencia de uso.

3.6.3 Cuadro o matriz de las variables

Tabla 3: Determinación de variables de investigación

Objetivos Específicos	Variable	Conceptualización	Operacionalización	Instrumento
1. Diagnosticar la situación actual respecto a la arquitectura tecnológica de la emisión de certificados académicos en la Universidad Internacional San Isidro Labrador.	Proceso de Emisión de Certificados	Secuencia de actividades y flujos de trabajo que la universidad sigue para generar, aprobar y entregar certificados académicos a sus estudiantes y egresados.	Se describirán los pasos actuales del proceso, identificando a los actores involucrados (CEU, Registro, etc.) y los documentos utilizados, desde la solicitud del estudiante hasta la entrega del certificado.	Documento Word
	Puntos de Vulnerabilidad	Debilidades o riesgos inherentes al sistema actual de emisión y verificación de certificados que lo exponen a fraude, errores o ineficiencias.	Se identificarán y se detallarán los puntos débiles del proceso actual, como la susceptibilidad a la falsificación, la dependencia de la intervención manual y los cuellos de botella en la verificación.	Hoja de cálculo de análisis de riesgos
	Percepción del Personal	Opiniones, experiencias y nivel de satisfacción de los empleados de la universidad involucrados en la	Se documentarán las perspectivas de los empleados del CEU y de Registro sobre la eficiencia, seguridad y desafíos del sistema actual.	Entrevistas a profundidad

		gestión de certificados.		
2. Realizar un estudio de viabilidad técnica y un análisis comparativo de plataformas blockchain, seleccionando la más adecuada y justificando su elección.	Criterios de Selección de Plataformas Blockchain	Atributos técnicos y económicos que determinan la idoneidad de una plataforma blockchain para la emisión de certificados académicos.	Se evaluarán y compararán plataformas como Ethereum, Solana y Hyperledger Fabric en función de su escalabilidad, costos de transacción, seguridad, ecosistema de desarrollo y tipo de red.	Hoja de cálculo de análisis comparativo
	Necesidades de Validación de Terceros	Requisitos y expectativas de empleadores y otras instituciones para la verificación de certificados de manera eficiente y confiable.	Se recolectarán datos sobre las dificultades actuales para verificar certificados y las características deseadas en un sistema de validación, como la velocidad y la facilidad de uso.	Encuesta a empresas
	Disponibilidad para la Adopción	La apertura y disposición de la gerencia y rectoría para considerar, financiar y adoptar una nueva tecnología.	Se evaluará la voluntad de la alta dirección para invertir en la solución, considerando su alineación con la misión y visión de la universidad.	Entrevistas a Gerencia y Rectoría
3. Diseñar la arquitectura tecnológica de un sistema de emisión y validación de certificados universitarios que utilice blockchain.	Módulo de Emisión en Blockchain	El componente de software propuesto que se integrará con el sistema actual para registrar certificados en la cadena de bloques.	Se describirán las funcionalidades del módulo, incluyendo el proceso de tokenización del certificado, la generación del hash y la firma digital.	Documento de diseño arquitectónico
	Interfaz de Validación con QR	La plataforma de usuario final y el mecanismo de	Se diseñará el flujo de usuario para la validación mediante	Diseño de interfaz de

		verificación que permite a terceros confirmar la autenticidad de un certificado.	un código QR, detallando la información que se mostrará y los pasos para verificar el certificado en la blockchain.	usuario (wireframes)
	Protocolo de Protección de Datos	Conjunto de reglas y mecanismos para asegurar que la información personal de los certificados sea accesible solo para partes autorizadas.	Se especificarán las medidas de seguridad para garantizar la privacidad, como la anonimización de datos en la cadena pública o el uso de claves de acceso restringido.	Documento de especificaciones de seguridad

Nota. Determinación de variables de investigación de acuerdo a los objetivos específicos. Fuente elaboración propia.

CAPÍTULO IV. ANÁLISIS DE RESULTADOS

4.1 Resultados de aplicación de entrevista a funcionarios de la Universidad (Autoridades académicas)

Este cuestionario tiene como objetivo recopilar la perspectiva de las altas autoridades sobre la problemática actual del fraude académico y la viabilidad, tanto estratégica como financiera, de implementar un sistema de validación de certificados basado en la tecnología Blockchain. Se adjunta entrevista como anexo número 1.

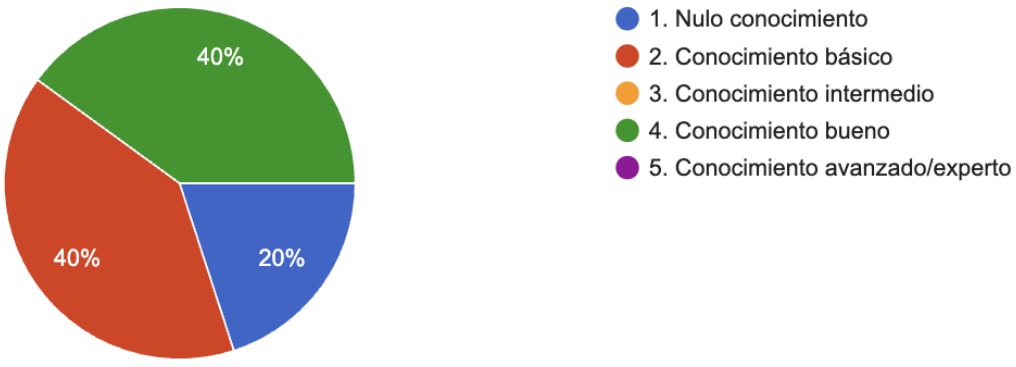
A continuación, se muestran los resultados obtenidos de la aplicación de dicha entrevista y las respuestas suministradas por los participantes. Cada gráfico refleja los niveles de conocimiento, percepción y experiencia de los entrevistados respecto a los temas clave abordados para la elaboración de esta propuesta.

Pregunta 1: ¿Cuál es el cargo que desempeña en la Universidad?

Esta pregunta es solamente de control y para determinar el cargo del funcionario, no hay resultados que analizar de la misma.

Pregunta 2: ¿Cuál es su nivel de conocimiento actual sobre la tecnología BlockChain?

Figura 6: Gráfico de respuestas a pregunta: ¿Cuál es su nivel de conocimiento actual sobre la tecnología BlockChain?



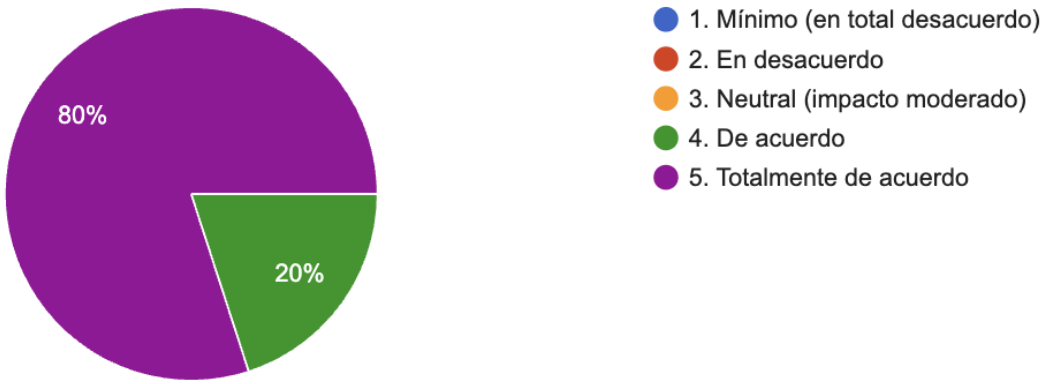
Nota: Elaboración propia

La distribución de las respuestas indica una base de conocimiento bastante dispersa pero con predominio en los niveles más bajos e intermedios. Específicamente, el 40% de los encuestados reportó tener un nivel de conocimiento bueno (el nivel más alto alcanzado en esta muestra), y otro 40% indicó tener

nonocimiento básico. El 20% restante admitió tener nulo conocimiento. Es notable que ninguno de los encuestados se identificó con los niveles de conocimiento intermedio o conocimiento avanzado/experto. Esto significa que el 80% de los participantes tiene al menos un conocimiento básico sobre Blockchain, mientras que la quinta parte carece de cualquier entendimiento.

Pregunta 3: ¿En qué medida considera que la adopción de Blockchain en la certificación posicionaría a la UISIL como una institución líder en innovación tecnológica?

Figura 7: Gráfico de respuestas a pregunta: ¿En qué medida considera que la adopción de Blockchain en la certificación posicionaría a la UISIL como una institución líder en innovación tecnológica?

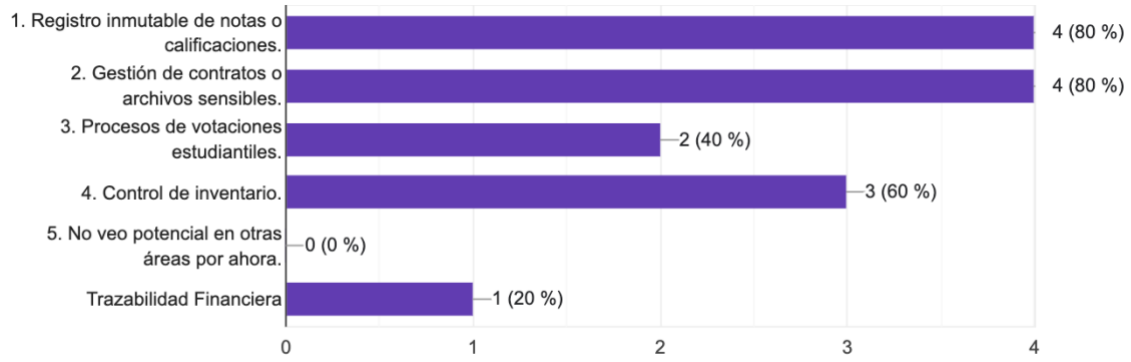


Nota: Elaboración propia

La distribución de las respuestas es totalmente positiva y enfática: un contundente 80% de los participantes seleccionó la opción "Totalmente de acuerdo", y el 20% restante optó por la categoría "De acuerdo", sin que ningún encuestado eligiera opciones neutrales o negativas. La conclusión es que existe un consenso total (100% de acuerdo) entre los encuestados de que la adopción de Blockchain para la certificación es un movimiento estratégico que posicionaría fuertemente a la UISIL como una institución líder en innovación tecnológica, lo que sugiere un alto nivel de apoyo y optimismo respecto al valor reputacional y tecnológico que la implementación de esta tecnología aportaría a la institución.

Pregunta 4: Además de certificados y títulos, ¿en qué otras áreas ve potencial para aplicar la tecnología Blockchain en la universidad?

Figura 8: Gráfico de respuestas a pregunta: Además de certificados y títulos, ¿en qué otras áreas ve potencial para aplicar la tecnología Blockchain en la universidad?



Nota: Elaboración propia

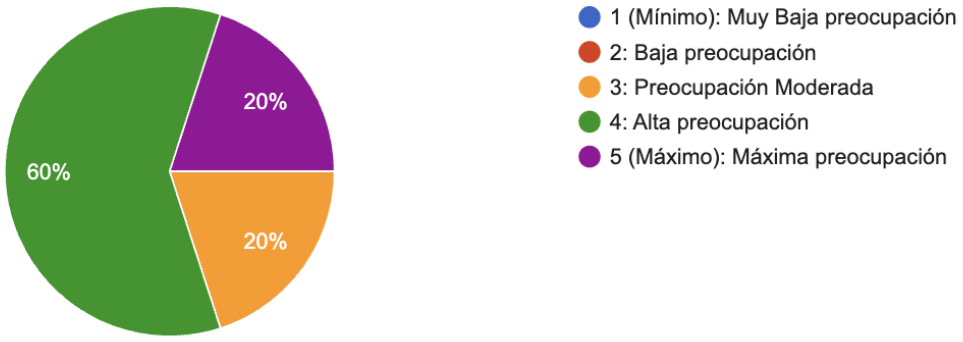
Según los funcionarios entrevistados, las áreas más destacadas para la aplicación potencial de Blockchain son el "Registro inmutable de notas o calificaciones" y la "Gestión de contratos o archivos sensibles", ambas seleccionadas por 4 de los 5 encuestados (80%). En un segundo plano, el "Control de inventario" también se consideró relevante, con 3 respuestas (60%).

Las categorías de "Procesos de votaciones estudiantiles" y una respuesta abierta de "Trazabilidad Financiera" recibieron un apoyo menor, con 2 (40%) y 1 (20%) respuesta, respectivamente.

Es significativo que ningún encuestado (0%) marcó la opción de "No veo potencial en otras áreas por ahora". La conclusión es que existe un fuerte consenso en que el mayor potencial de Blockchain reside en la seguridad e inmutabilidad de los datos académicos críticos y la documentación administrativa (notas y archivos sensibles), y que la totalidad de los encuestados ve potencial en múltiples áreas de aplicación universitaria más allá de la certificación.

Pregunta 5: ¿Cuál es su nivel de preocupación respecto al riesgo actual o potencial de fraude (falsificación/alteración) con certificados académicos?

Figura 9: Gráfico de respuestas a pregunta: ¿Cuál es su nivel de preocupación respecto al riesgo actual o potencial de fraude (falsificación/alteración) con certificados académicos?



Nota: Elaboración propia

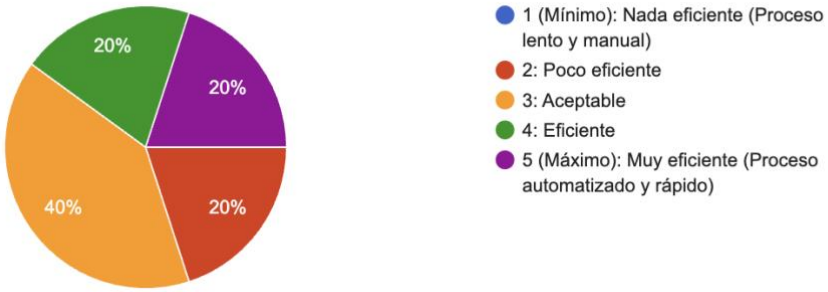
La figura anterior ilustra el nivel de preocupación de los 5 entrevistados respecto al riesgo actual o potencial de fraude (falsificación/alteración) con certificados académicos. Los resultados muestran que la preocupación es predominantemente alta.

El 60% de los participantes manifestó tener "Alta preocupación", y un significativo 20% reportó tener el nivel máximo de "Máxima preocupación". Solo el 20% restante indicó tener una "Preocupación Moderada", y ningún encuestado seleccionó los niveles de "Baja preocupación" o "Muy Baja preocupación".

Se concluye que existe una alta inquietud generalizada entre los encuestados sobre la vulnerabilidad de los certificados académicos al fraude, ya que el 80% de la muestra reporta un nivel de preocupación alto o máximo, lo que sugiere que existe una necesidad percibida de soluciones tecnológicas robustas, como Blockchain, para mitigar este riesgo.

Pregunta 6: ¿Qué tan eficiente y rápida considera que es la Universidad en la verificación de certificados ante solicitudes de terceros (ej. empleadores o instituciones educativas externas)?

Figura 10: Gráfico de respuestas a pregunta: ¿Qué tan eficiente y rápida considera que es la Universidad en la verificación de certificados ante solicitudes de terceros (ej. empleadores o instituciones educativas externas)?



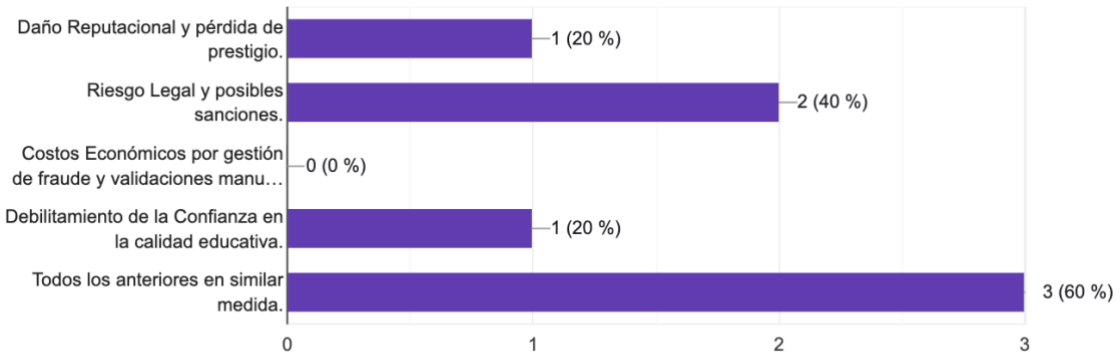
Nota: Elaboración propia

Los resultados muestran una distribución mixta, con opiniones que varían desde la ineficiencia hasta la máxima eficiencia. El 40% de los encuestados considera el proceso como "Aceptable", representando la moda de las respuestas. Sin embargo, el 20% lo considera "Poco eficiente", y otro 20% lo valora como "Eficiente". El restante 20% califica el proceso como "Muy eficiente (Proceso automatizado y rápido)". Es relevante que ningún encuestado lo considere "Nada eficiente".

La conclusión es que, si bien una parte significativa de los encuestados (40%) considera la eficiencia de la verificación como aceptable, existe una división en la percepción de su rapidez: el 40% lo ve como eficiente o muy eficiente, mientras que el 20% lo considera poco eficiente. Esta dispersión sugiere que el proceso actual de verificación tiene margen de mejora para ser percibido como consistentemente rápido y eficiente por la mayoría, lo que justificaría la búsqueda de soluciones automatizadas, como la que podría ofrecer Blockchain.

Pregunta 7: ¿Cuál cree que es el principal impacto que el fraude académico tiene o podría tener sobre la institución?

Figura 11: Gráfico de respuestas a pregunta: ¿Cuál cree que es el principal impacto que el fraude académico tiene o podría tener sobre la institución?



Nota: Elaboración propia

El impacto más frecuentemente citado es la combinación de todos los riesgos: el 60% de los encuestados seleccionó la opción "Todos los anteriores en similar medida". De las opciones individuales, "Riesgo Legal y posibles sanciones" fue la más elegida, con 2 respuestas (40%).

Las opciones de "Daño Reputacional y pérdida de prestigio" y "Debilitamiento de la Confianza en la calidad educativa" fueron seleccionadas por 1 encuestado (20%) cada una, mientras que nadie (0%) consideró los "Costos Económicos por gestión de fraude y validaciones manuales" como el impacto principal.

La conclusión es que los encuestados perciben el fraude académico como un riesgo sistémico y multifacético, donde la mayoría cree que el impacto se distribuye simultáneamente en el daño a la reputación, el riesgo legal y la confianza en la calidad educativa.

Pregunta 8: Según su criterio, mencione la característica más importante que debe tener un nuevo sistema de validación para combatir drásticamente el fraude y mejorar la confianza.

Tabla 4: Respuestas a la pregunta: Según su criterio, mencione la característica más importante que debe tener un nuevo sistema de validación para combatir drásticamente el fraude y mejorar la confianza.

Perfil	Respuesta
Rectoría	Efectividad.
Gerencia Administrativa	Rápido, seguro y que permita garantizar la veracidad de la información.
Dirección de Registro	La verificación de autenticación continua.
Dirección de CEU	Que los datos registrados no puedan modificarse ni alterarse, y que cualquier intento de cambio sea detectado de inmediato.
Coordinación de CEU	Verificación de identidad por algún medio.

Nota: Elaboración propia

La mayoría de las respuestas se concentran en atributos clave de seguridad e inmutabilidad. Dos respuestas se centran explícitamente en la inmutabilidad y la veracidad de los datos, con la frase "Que los datos registrados no puedan modificarse ni alterarse, y que cualquier intento de cambio sea detectado de inmediato" siendo la más descriptiva. Otra respuesta enfatiza una combinación de atributos: "Rápido, seguro y que permita garantizar la veracidad de la información".

Las respuestas restantes son más generales, citando la "Efectividad", la "verificación de identidad por algún medio", y "La verificación de autenticación continua".

Se concluye de estas respuestas, que la característica más importante y deseada para un nuevo sistema de validación es la inmutabilidad de los registros académicos, es decir, la garantía de que la información no pueda ser falsificada ni alterada, combinada con la rapidez y la seguridad del proceso, lo cual coincide directamente con los beneficios centrales que ofrece una tecnología como Blockchain en la emisión de certificados.

Pregunta 9: Considerando las prioridades institucionales, ¿qué nivel de prioridad asignaría a la asignación de un presupuesto para este proyecto de ciberseguridad basado en Blockchain?

Figura 12: Gráfico de respuestas a pregunta: Considerando las prioridades institucionales, ¿qué nivel de prioridad asignaría a la asignación de un presupuesto para este proyecto de ciberseguridad basado en Blockchain?

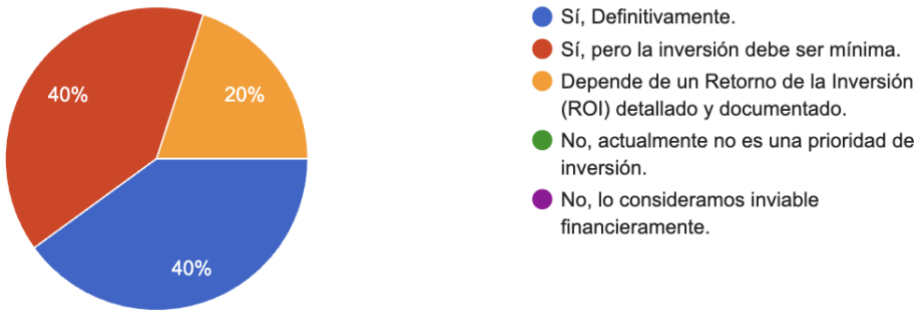
Nota: Elaboración propia

La distribución de respuestas muestra un fuerte enfoque en las prioridades más altas. El 40% de los encuestados asignó una "Alta prioridad" al proyecto, y otro 20% le dio la "Máxima prioridad (Debe ser presupuestado y ejecutado este año)". El 20% restante consideró una "Prioridad Media (Debe ser considerado)", y otro 20% lo situó en una "Prioridad Modesta". Es importante destacar que ningún encuestado lo consideró de "Baja prioridad".

Se concluye que existe una percepción mayoritaria (60%) de que el proyecto de ciberseguridad basado en Blockchain para la certificación debe ser una prioridad alta o máxima en la agenda institucional, lo que se alinea con la alta preocupación por el fraude y el reconocimiento del potencial de esta tecnología observado en los gráficos anteriores, sugiriendo un claro apoyo a la asignación de recursos.

Pregunta 10: ¿Estaría su departamento dispuesto a evaluar una inversión inicial que prometa reducir costos a largo plazo (trámites manuales, litigios) y mitigar el riesgo de fraude?

Figura 13: Gráfico de respuestas a pregunta: ¿Estaría su departamento dispuesto a evaluar una inversión inicial que prometa reducir costos a largo plazo (trámites manuales, litigios) y mitigar el riesgo de fraude?



Nota: Elaboración propia

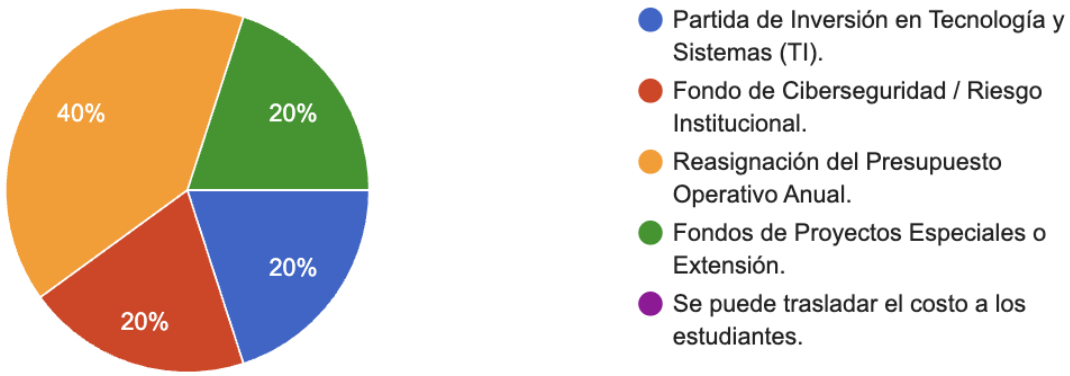
Las respuestas reflejan una clara disposición a la inversión, aunque con diferentes condiciones. Un 40% de los encuestados respondió "Sí, Definitivamente", mostrando el mayor nivel de compromiso. Otro 40% respondió "Sí, pero la inversión debe ser mínima", indicando una disposición condicionada a la contención de costos. El 20% restante indicó que "Depende de un Retorno de la Inversión (ROI) detallado y documentado".

Es importante destacar que ningún encuestado seleccionó las opciones negativas ("No, actualmente no es una prioridad de inversión" o "No, lo consideramos inviable financieramente").

La conclusión es que existe un consenso total (100% de disposición) para evaluar la inversión en una solución que reduzca costos y mitigue el fraude. No obstante, la mayoría de los encuestados (60% al sumar "mínima" y "depende del ROI") necesitaría ver una propuesta financiera sólida, que demuestre un ROI claro y justifique la inversión inicial, antes de proceder con el proyecto.

Pregunta 11: ¿De qué partidas presupuestarias o fuentes se podrían obtener fondos para cubrir los costos de desarrollo, implementación y mantenimiento del sistema?

Figura 14: Gráfico de respuestas a pregunta: ¿De qué partidas presupuestarias o fuentes se podrían obtener fondos para cubrir los costos de desarrollo, implementación y mantenimiento del sistema?



Nota: Elaboración propia

La respuesta más común, seleccionada por el 40% de los encuestados, es la "Reasignación del Presupuesto Operativo Anual". Las otras opciones se distribuyen de manera uniforme: el 20% sugiere la "Partida de Inversión en Tecnología y Sistemas (TI)", otro 20% indica el "Fondo de Ciberseguridad / Riesgo Institucional", y el 20% restante propone usar "Fondos de Proyectos Especiales o Extensión". Es significativo que ningún encuestado consideró la opción de "Trasladar el costo a los estudiantes".

La conclusión es que, si bien hay una variedad de fuentes potenciales identificadas, la reasignación de fondos operativos existentes es percibida como la fuente más viable o preferida para cubrir los costos del proyecto de Blockchain, sugiriendo una preferencia por financiar la innovación internamente mediante la reestructuración presupuestaria.

Pregunta 12: ¿Cuál será el principal desafío u obstáculo operativo que enfrentará su área (Registro o CEU) con la implementación de este nuevo sistema de certificación?

Tabla 5: Respuestas a la pregunta: ¿Cuál será el principal desafío u obstáculo operativo que enfrentará su área (Registro o CEU) con la implementación de este nuevo sistema de certificación?

Perfil	Respuesta
Rectoría	El entendimiento de los procesos Blockchain
Gerencia Administrativa	Resistencia al cambio y/o cumplimiento de normativa actual de los entes supervisores.
Dirección de Registro	El principal desafío operativo será la dependencia del ente regulador CONESUP, ya que este mantiene sistemas internos propios, con procesos, formatos y requisitos que no necesariamente están alineados con el nuevo sistema de certificación que la universidad implementaría
Dirección de CEU	Resistencia al cambio y/o cumplimiento de normativa actual de los entes supervisores.
Coordinación de CEU	Capacitar al personal y adaptar los procesos para usar correctamente el nuevo sistema sin afectar la operación diaria.

Nota: Elaboración propia

Las respuestas revelan que los obstáculos se perciben principalmente en la esfera organizacional y regulatoria. Dos desafíos clave identificados son la "Resistencia al cambio y/o cumplimiento de normativa actual de los entes supervisores" y la "dependencia del ente regulador CONESUP" cuyos sistemas internos pueden no estar alineados, señalando el factor regulatorio como un riesgo importante. Además, se menciona la necesidad de "Capacitar al personal y adaptar los procesos", destacando el desafío interno de la gestión del cambio. Otro

encuestado menciona específicamente "El entendimiento de los procesos Blockchain".

La conclusión es que el principal obstáculo operativo percibido para la implementación del nuevo sistema de certificación no es tecnológico, sino la complejidad de la alineación regulatoria (CONESUP) y la gestión del cambio interno, incluyendo la capacitación del personal y la superación de la resistencia al nuevo modelo.

Pregunta 13: ¿Qué medidas sugeriría para asegurar la aceptación y el uso de estos certificados digitales por parte de empleadores, gobiernos y otras instituciones externas?

Tabla 6: Respuestas a la pregunta: ¿Cuál será el principal desafío u obstáculo operativo que enfrentará su área (Registro o CEU) con la implementación de este nuevo sistema de certificación?

Perfil	Respuesta
Rectoría	Es un proceso difícil que se debe de presentar como un proyecto innovador en la Asamblea Legislativa como ejemplo yo propuse algo parecido en el CONESUP y no fue entendido en su momento.
Gerencia Administrativa	Cambios normativos a nivel de Conesup, es el primer paso.
Dirección de Registro	Garantizar que los certificados cumplan con normativas nacionales Permitir verificación sin necesidad de registrarse o descargar aplicaciones Lanzar una campaña de comunicación institucional explicando beneficios y seguridad de los certificados Ofrecer soporte técnico para instituciones externas

Dirección de CEU	El personal deberá aprender y acostumbrarse a un nuevo sistema digital y sus procesos.
Coordinación de CEU	Informarlos bien de como funciona esta metodología y lo práctico que sería verificarlos y tenerlos a la mano

Nota: Elaboración propia

Las sugerencias se centran fuertemente en dos áreas: legalidad/normativa y comunicación/facilidad de uso. La medida más fundamental citada es lograr "Cambios normativos a nivel de CONESUP" y "Garantizar que los certificados cumplan con normativas nacionales". Esto se complementa con la necesidad de una campaña de comunicación robusta para informar sobre los beneficios y la seguridad, así como asegurar la facilidad de uso, proponiendo "Permitir verificación sin necesidad de registrarse o descargar aplicaciones" y "Ofrecer soporte técnico". También se enfatiza el desafío político: "Es un proceso difícil que se debe presentar como un proyecto innovador en la Asamblea Legislativa".

La conclusión es que la aceptación del nuevo sistema de certificación digital depende completamente de dos factores dependientes entre sí: primero, la validación legal y normativa por parte de los entes reguladores (CONESUP principalmente), y segundo, una estrategia de comunicación clara combinada con una experiencia de usuario externa (verificación) simple y directa.

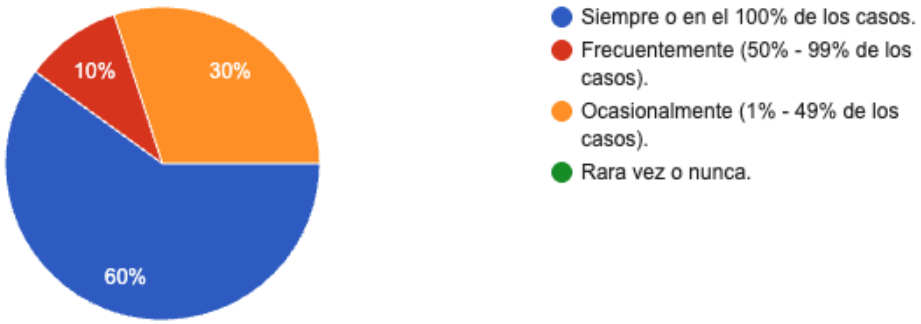
4.2 Resultados de aplicación de entrevista a empresas (posibles empleadores)

Este cuestionario tiene como objetivo recolectar información sobre la experiencia actual de las empresas en la validación de credenciales académicas y evaluar el interés y la viabilidad de implementar un sistema de verificación instantáneo y seguro basado en tecnología Blockchain para los certificados emitidos por la Universidad Internacional San Isidro Labrador. Se adjunta cuestionario como anexo número 2.

A continuación, se muestran los resultados obtenidos de la aplicación de dicho cuestionario y las respuestas suministradas por los participantes. Cada gráfico refleja los niveles de conocimiento, percepción y experiencia de los entrevistados respecto a los temas clave abordados para la elaboración de esta propuesta.

Pregunta 1: ¿Con qué frecuencia su empresa verifica los certificados, títulos o diplomas de los postulantes o empleados?

Figura 15: Gráfico de respuestas a pregunta: ¿Con qué frecuencia su empresa verifica los certificados, títulos o diplomas de los postulantes o empleados?



Nota: Elaboración propia

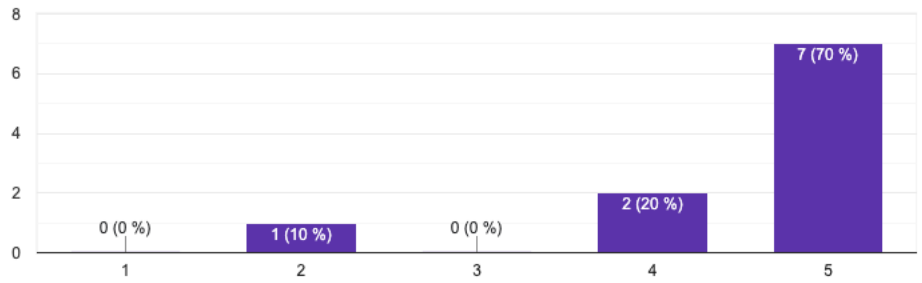
El análisis de las respuestas recibidas indica que la mayoría de las empresas encuestadas tienen una política estricta o de alta frecuencia en la verificación de los certificados, títulos o diplomas de sus postulantes o empleados, con un 60% de las organizaciones afirmando realizar esta verificación Siempre o en el 100% de los casos.

Sin embargo, la frecuencia disminuye significativamente para el resto de la muestra: el 30% lo hace solo Ocasionalmente (entre el 1% y el 49% de los casos), lo que sugiere una aplicación irregular y discrecional, y un 10% restante verifica las credenciales Frecuentemente (entre el 50% y el 99% de los casos).

En conclusión, si bien la mitad más uno de los encuestados demuestra un compromiso total con la diligencia debida en la verificación de credenciales, el 40% restante no garantiza la autenticidad de los títulos en todos sus procesos, lo cual representa una vulnerabilidad potencial en la gestión de recursos humanos para una porción significativa de las empresas.

Pregunta 2: En una escala del 1 al 5, ¿qué tan importante considera el proceso de verificación de certificados académicos para su proceso de contratación? (Siendo 1: Nada importante y 5: Crítico)

Figura 16: Gráfico de respuestas a pregunta: En una escala del 1 al 5, ¿qué tan importante considera el proceso de verificación de certificados académicos para su proceso de contratación? (Siendo 1: Nada importante y 5: Crítico)



Nota: Elaboración propia

Analizando las repuestas recibidas, se puede notar un consenso abrumadoramente alto sobre su valor.

Específicamente, el **70%** de los encuestados calificó el proceso con un 5 (Crítico), lo que indica que lo consideran una función esencial y no negociable en su proceso de selección.

Sumando a esto, un **20%** adicional calificó la importancia con un 4, elevando el total de respuestas que consideran el proceso "Importante" o "Crítico" al 90%. Solo una empresa (el 10%) lo calificó con un 2.

En conclusión, la mayoría de las empresas participantes perciben la verificación de certificados académicos como una tarea de alta o máxima prioridad, reflejando una clara conciencia sobre la necesidad de mitigar riesgos y asegurar la idoneidad y autenticidad de las credenciales de los postulantes.

Pregunta 3: ¿Ha detectado o sospechado de certificados académicos fraudulentos (falsificados o alterados) en los últimos 3 años?

Figura 17: Gráfico de respuestas a pregunta: ¿Ha detectado o sospechado de certificados académicos fraudulentos (falsificados o alterados) en los últimos 3 años?

Nota: Elaboración propia

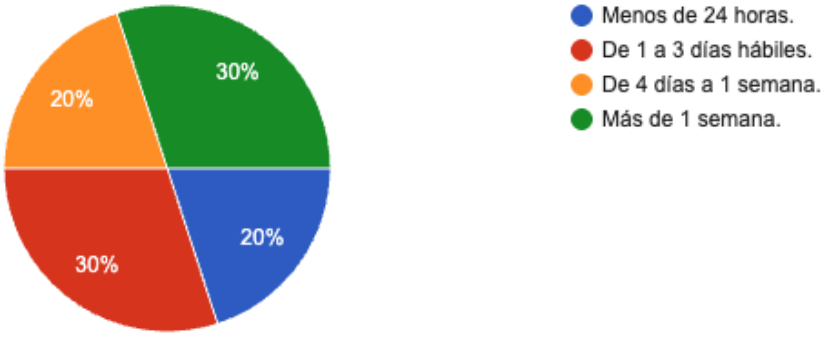
El análisis de las 10 respuestas relativas a la detección o sospecha de certificados académicos fraudulentos en los últimos tres años muestra una división clara entre las empresas.

El 70% de los encuestados reportó No haber detectado ni sospechado nunca de fraude en las credenciales. Sin embargo, un 30% de las empresas Sí ha tenido sospechas, pero sin que se hayan confirmado casos de fraude.

Aunque la mayoría de las empresas encuestadas no ha encontrado evidencia de fraude, el hecho de que casi un tercio de ellas haya tenido sospechas sin confirmar indica que la amenaza de fraude existe y que las medidas de verificación podrían estar generando alerta, aunque el proceso de confirmación y documentación de estos casos no se haya completado o no se considere público.

Pregunta 4: Cuando realiza una verificación con una institución educativa, ¿cuál es el tiempo promedio de respuesta que experimenta?

Figura 18: Gráfico de respuestas a pregunta: Cuando realiza una verificación con una institución educativa, ¿cuál es el tiempo promedio de respuesta que experimenta?



Nota: Elaboración propia

El análisis de las 10 respuestas relativas al tiempo promedio de respuesta al verificar certificados con una institución educativa revela que existe una distribución equitativa, pero predominantemente lenta, de los tiempos de respuesta. Solamente el 20% de las empresas experimenta una respuesta rápida, recibiendo la información en Menos de 24 horas.

En contraste, la mayoría de los encuestados reporta demoras que se extienden más allá de los tres días hábiles: el 30% espera de 1 a 3 días hábiles, otro 20% espera de 4 días a 1 semana, y el 30% restante experimenta el tiempo más largo, con demoras de más de 1 semana.

En conclusión, solo una minoría de empresas logra una verificación eficiente en menos de un día, mientras que una mayoría considerable (80%) enfrenta tiempos de espera que ralentizan el proceso de contratación, ya que deben esperar entre uno y más de siete días para obtener la confirmación académica.

Pregunta 5: ¿Cuál de los siguientes es el principal problema que enfrenta su empresa al verificar certificados académicos?

Figura 19: Gráfico de respuestas a pregunta: ¿Cuál de los siguientes es el principal problema que enfrenta su empresa al verificar certificados académicos?

Nota: Elaboración propia

El análisis de las 10 respuestas sobre el principal problema que enfrentan las empresas al verificar certificados académicos revela una causa fundamental del cuello de botella en este proceso.

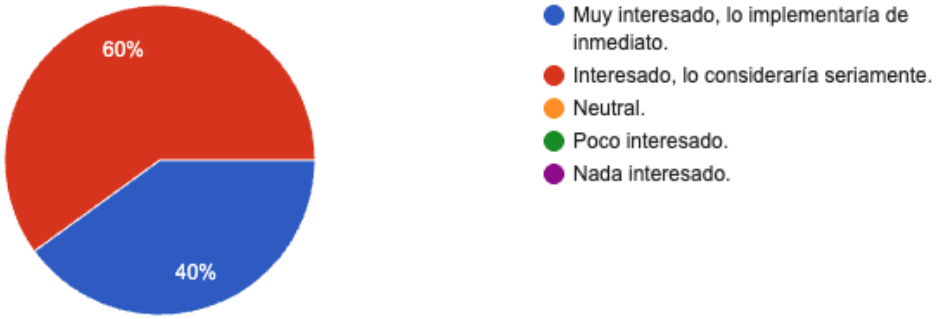
Una mayoría contundente del 60% de los encuestados identifica las Demoras en la respuesta de las instituciones como el problema más crítico, lo que concuerda directamente con los hallazgos de la pregunta anterior sobre los largos tiempos de espera.

Otros problemas son identificados en menor medida: el Alto costo administrativo/tiempo invertido es el principal obstáculo para el 20% de las empresas, mientras que el Alto riesgo de fraude/falsificación y la Falta de un proceso estandarizado y claro comparten la preocupación con un 10% cada uno.

En conclusión, la ineficiencia operativa generada por la lentitud de las instituciones educativas es, con diferencia, el mayor desafío que enfrentan las empresas en la verificación de credenciales. La preocupación por el fraude y la estandarización, aunque presentes, son problemas secundarios frente a la barrera impuesta por la falta de agilidad en las respuestas externas.

Pregunta 6: Si existiera un sistema que le permitiera verificar la autenticidad de un certificado de forma instantánea y en línea (24/7), ¿qué tan interesado estaría en utilizarlo?

Figura 20: Gráfico de respuestas a pregunta: Si existiera un sistema que le permitiera verificar la autenticidad de un certificado de forma instantánea y en línea (24/7), ¿qué tan interesado estaría en utilizarlo?



Nota: Elaboración propia

El análisis de las 10 respuestas sobre el interés en implementar un sistema de verificación de autenticidad de certificados instantáneo y en línea (24/7) revela una aceptación prácticamente total y urgente por parte de las empresas.

El 40% de los encuestados manifestó estar Muy interesado e implementaría el sistema de inmediato, lo que subraya la necesidad crítica de resolver los problemas de demora ya identificados. El 60% restante indicó estar Interesado y lo consideraría seriamente. En conjunto, el 100% de las empresas encuestadas mostró un grado significativo de interés en esta solución tecnológica.

En conclusión, este resultado confirma la existencia de una demanda insatisfecha de herramientas que permitan la verificación ágil, lo cual es coherente con que las demoras institucionales hayan sido identificadas como el principal problema. La disposición unánime de las empresas a adoptar un sistema instantáneo y en línea sugiere que esta solución sería altamente efectiva para eliminar el cuello de botella operativo en los procesos de recursos humanos.

Pregunta 7: ¿Cuál es el atributo más valioso que buscaría en un nuevo sistema de validación de certificados?

Figura 21: Gráfico de respuestas a pregunta: ¿Cuál es el atributo más valioso que buscaría en un nuevo sistema de validación de certificados?

Nota: Elaboración propia

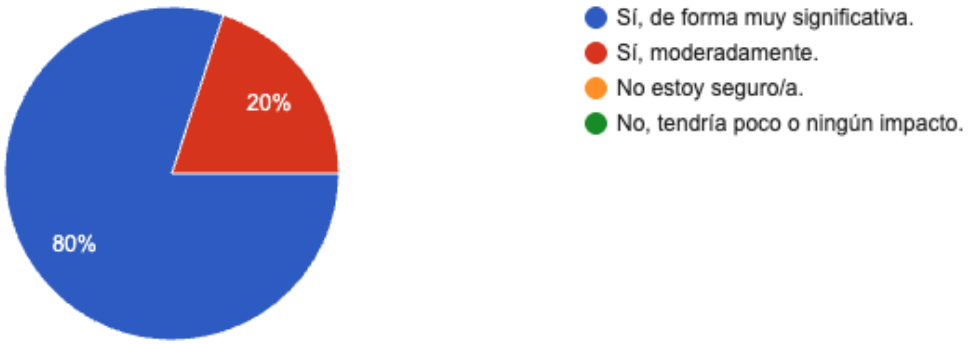
El análisis de las 10 respuestas relativas al atributo más valioso que se buscaría en un nuevo sistema de validación de certificados establece claramente que la confiabilidad es la prioridad indiscutible. Una mayoría sustancial del 60% de las empresas encuestadas seleccionó la Confiabilidad/Seguridad (Garantía de que el certificado no es fraudulento) como el atributo más valioso.

En segundo lugar, y en coherencia con la queja principal sobre las demoras, la Rapidez/Inmediatez de la verificación es considerada el atributo más valioso por el 20% de la muestra. Los factores operativos y la profundidad de la información se reparten el 20% restante: el 10% prioriza la Facilidad de uso, y el otro 10% valora más el Acceso a información detallada sobre el logro académico.

En conclusión, a pesar de que la lentitud en la respuesta es el principal problema operativo, la principal motivación y exigencia para cualquier nueva solución es la seguridad y la garantía de autenticidad. Esto sugiere que las empresas están dispuestas a adoptar tecnologías que, ante todo, eliminen el riesgo de fraude, siendo la velocidad un factor de alto valor, pero secundario a la fiabilidad.

Pregunta 8: ¿Cree que la facilidad y rapidez en la verificación de credenciales académicas impactaría positivamente en la eficiencia de sus procesos de contratación?

Figura 22: Gráfico de respuestas a pregunta: ¿Cree que la facilidad y rapidez en la verificación de credenciales académicas impactaría positivamente en la eficiencia de sus procesos de contratación?



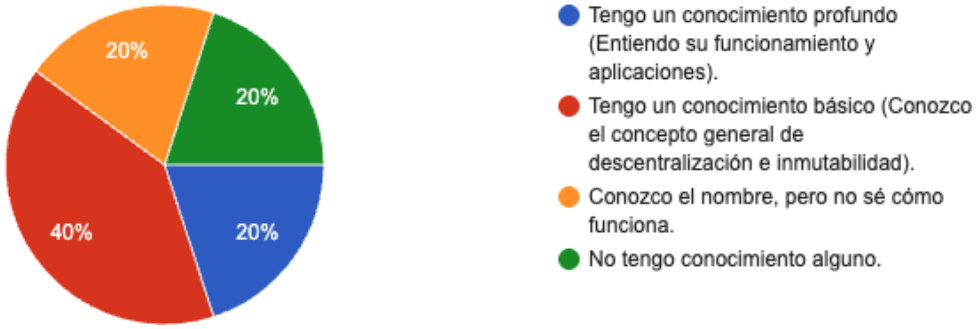
Nota: Elaboración propia

El análisis de las 10 respuestas sobre si la facilidad y rapidez en la verificación de credenciales impactarían positivamente en la eficiencia de los procesos de contratación revela un consenso total y de alta intensidad. El 80% de los encuestados cree que el impacto sería Sí, de forma muy significativa, mientras que el 20% restante considera que el impacto sería Sí, moderadamente. Ningún encuestado mostró incertidumbre o creyó que el impacto sería nulo o bajo.

En conclusión, la totalidad de las empresas encuestadas está convencida de que la mejora en la velocidad y simplicidad de la verificación se traduce directamente en una mejora tangible y significativa de la eficiencia en sus procesos de contratación. Este resultado final valida la necesidad de buscar soluciones tecnológicas rápidas, ya que las empresas no solo las desean (Pregunta 6), sino que están seguras de su beneficio operativo y estratégico.

Pregunta 9: ¿Qué tanto conocimiento tiene sobre la tecnología Blockchain (Cadena de Bloques)?

Figura 23: Gráfico de respuestas a pregunta: ¿Qué tanto conocimiento tiene sobre la tecnología Blockchain (Cadena de Bloques)?



Nota: Elaboración propia

El análisis de las 10 respuestas sobre el nivel de conocimiento de la tecnología Blockchain (Cadena de Bloques) revela una distribución variada en el entendimiento de esta tecnología entre las empresas encuestadas.

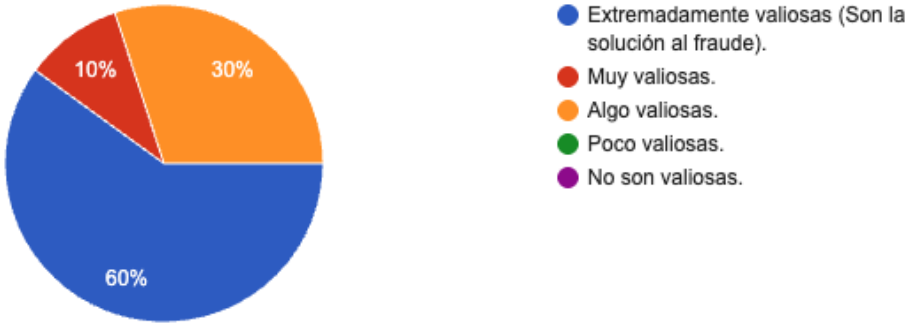
La mayoría, con un 40%, se sitúa en un nivel de Conocimiento básico, lo que implica que conocen el concepto general de descentralización e inmutabilidad. Sumando a este grupo, el 20% tiene un Conocimiento profundo (entendiendo su funcionamiento y aplicaciones). Esto significa que el 60% de los encuestados tiene al menos un conocimiento funcional de la tecnología.

Por otro lado, un 20% de la muestra solo conoce el nombre, pero no sabe cómo funciona, y otro 20% reporta no tener conocimiento alguno.

En conclusión, si bien la mitad más uno de los encuestados posee un nivel de conocimiento que permite entender las bases de Blockchain, existe una brecha significativa donde el 40% tiene un conocimiento superficial o nulo. Este nivel de conocimiento mixto es relevante ya que la solución que se pretende presentar está basada en la tecnología de blockchain.

Pregunta 10: La tecnología Blockchain garantiza la inmutabilidad (un registro no puede ser alterado) y la descentralización de los datos. ¿Qué tan valiosas son estas características para la verificación de un certificado académico?

Figura 24: Gráfico de respuestas a pregunta: La tecnología Blockchain garantiza la inmutabilidad (un registro no puede ser alterado) y la descentralización de los datos. ¿Qué tan valiosas son estas características para la verificación de un certificado académico?



Nota: Elaboración propia

El análisis de las 10 respuestas sobre cuán valiosas son la inmutabilidad y la descentralización de Blockchain para la verificación de certificados académicos revela un reconocimiento muy alto de su valor anti-fraude.

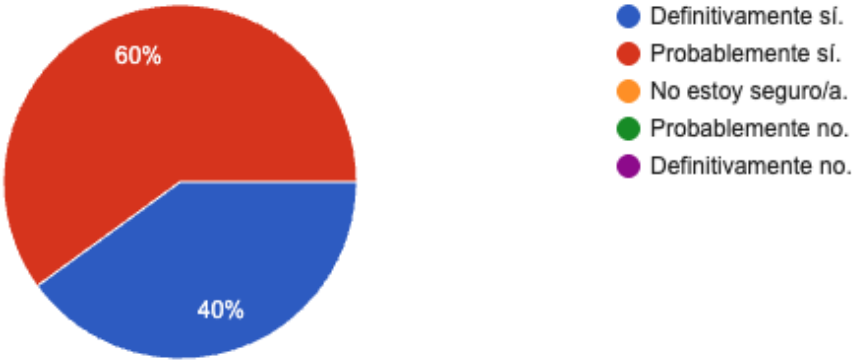
Una clara mayoría del 60% de las empresas considera estas características como Extremadamente valiosas (Son la solución al fraude). Un 10% adicional las considera Muy valiosas, y el 30% restante las ve como Algo valiosas. Es importante destacar que ningún encuestado consideró estas características como poco o nada valiosas.

En conclusión, los encuestados que poseen algún nivel de conocimiento de Blockchain (Pregunta 9) perciben fuertemente que sus atributos centrales abordan directamente su principal exigencia para un nuevo sistema de verificación: la confiabilidad y la seguridad (Pregunta 7).

Esta percepción refuerza el interés por soluciones tecnológicas que garanticen un registro inalterable de las credenciales y certificados académicos, posicionando la inmutabilidad como un requisito clave para combatir el fraude en el sector.

Pregunta 11: Suponiendo que un sistema de validación basado en Blockchain cumple con todas las leyes de protección de datos, ¿su empresa estaría dispuesta a utilizar este tipo de tecnología para la verificación de certificados?

Figura 25: Gráfico de respuestas a pregunta: Suponiendo que un sistema de validación basado en Blockchain cumple con todas las leyes de protección de datos, ¿su empresa estaría dispuesta a utilizar este tipo de tecnología para la verificación de certificados?



Nota: Elaboración propia

El análisis de las 10 respuestas sobre la disposición de las empresas a utilizar un sistema de validación basado en Blockchain (asumiendo el cumplimiento de la protección de datos) revela una aceptación total y muy alta de la tecnología. El 40% de los encuestados afirmó que Definitivamente sí utilizaría este tipo de tecnología, lo que indica un fuerte convencimiento en la solución. El 60% restante indicó que Probablemente sí la usaría. Ninguna empresa mostró indecisión, duda o rechazo.

En conclusión, este resultado sella el ciclo del interés, la necesidad y la voluntad de adopción. La unanimidad en la disposición a usar Blockchain para la verificación de certificados, especialmente al estar garantizada la protección de datos, confirma que la tecnología es vista como la solución viable y preferida para resolver el dilema central del estudio: la necesidad de máxima confiabilidad y seguridad contra el fraude, combinada con la urgencia de eliminar las demoras operativas.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Objetivo específico N1: Diagnosticar la situación actual respecto a la arquitectura tecnológica de la emisión de certificados académicos en la Universidad Internacional San Isidro Labrador.

Este objetivo se logró al investigar a profundidad el proceso interno de la universidad mediante la aplicación de la Entrevista a Funcionarios y Autoridades Académicas. El diagnóstico se centró en mapear el “estado del arte” de la certificación, revelando varios puntos críticos.

Se confirmó que el proceso actual depende de formatos físicos y verificación manual, lo que se traduce en una alta vulnerabilidad al fraude (falsificación y alteración de documentos) y una baja eficiencia operativa.

Específicamente, se logró cuantificar la percepción de la demora y la complejidad para que terceros (en este caso, empleadores) verifiquen la autenticidad de un título. Los hallazgos de esta etapa establecieron la justificación crítica para el proyecto: la necesidad de un sistema que eliminara el riesgo de fraude y agilizara definitivamente la verificación.

Sin embargo, es necesario mencionar que el proceso de emisión de certificados por blockchain, solamente funcionaría en los generados por el departamento del CEU, ya que los académicos universitarios, dependen del Consejo Nacional de Educación, y existe una legislación al respecto, lo cual imposibilita a la Universidad en la toma de decisiones sobre este proceso, y la obliga a apegarse a lo establecido a nivel nacional.

Objetivo específico N2: Realizar un estudio de viabilidad técnica y un análisis comparativo de plataformas blockchain, seleccionando la más adecuada y justificando su elección para un futuro prototipo o implementación en un entorno universitario.

Este objetivo se satisfizo mediante una doble aproximación: la viabilidad de mercado y el análisis técnico comparativo. La viabilidad de mercado fue confirmada a través de la Encuesta a Empresas (Posibles Empleadores), donde se demostró la necesidad y el deseo del sector externo de adoptar la solución.

El 100% de las empresas encuestadas manifestaron una gran insatisfacción con los tiempos de respuesta del sistema actual, y más del 90% expresaron una alta disposición a utilizar una tecnología basada en blockchain para la verificación, siempre que garantizara la protección de datos.

Este resultado validó la hipótesis central de que el mercado laboral valora enormemente la inmutabilidad, la seguridad y la inmediatez.

Simultáneamente, se llevó a cabo el análisis comparativo de plataformas blockchain líderes como Ethereum, Solana y Hyperledger Fabric, evaluando sus características en cuanto a escalabilidad, costos de transacción (*gas fees*), modelo de permisos (público vs. privado) y seguridad.

Este análisis técnico condujo a la selección justificada de la plataforma más adecuada para el entorno universitario, como lo es HyperLedger, por su vasta documentación, su inmutabilidad garantizada y su popularidad en el mercado de las redes blockchain, confirmando así la viabilidad técnica de la implementación.

Objetivo específico N3: Diseñar la arquitectura tecnológica de un sistema de emisión y validación de certificados universitarios que utilice blockchain para asegurar la inmutabilidad y autenticidad de los certificados, previniendo la falsificación y el fraude.

El diseño de la arquitectura es la culminación práctica de las fases de diagnóstico y viabilidad. El diseño propuesto se centra en la integración y la funcionalidad.

Se propone una arquitectura que incluye un Módulo de Emisión en Blockchain que se acopla al Sistema de Gestión de Procesos (ERP) ya existente de la universidad. La función central de este módulo es generar y registrar la huella

digital (hash) de cada certificado en la cadena de bloques, sin necesidad de almacenar la información personal completa en ella.

Para la validación externa, se propone el diseño una Interfaz de Validación con Código QR, la cual se coloca en el certificado digital (PDF). Al escanear este código, el tercero es dirigido a una plataforma web que consulta la blockchain de forma instantánea, verificando la autenticidad y los metadatos esenciales del documento.

Este diseño resuelve directamente la ineficiencia del diagnóstico (Objetivo 1) y cumple con las demandas de inmediatez y seguridad expresadas por las empresas (Objetivo 2), completando exitosamente el ciclo del proyecto.

5.2 Recomendaciones

1. Aprobación e Inversión Inicial del Proyecto

La primera y más importante recomendación es la aprobación formal de la propuesta y la asignación presupuestaria inicial. La Rectoría y la Gerencia Financiera deben evaluar los resultados del estudio de viabilidad, que confirman una necesidad de mercado y una alta aceptación, para dar luz verde a la iniciativa en el corto plazo (0-3 meses).

Esta decisión es fundamental para superar las etapas iniciales del proyecto y abordar la variable de Disponibilidad para la Adopción. Es necesario que la inversión inicial no solo cubra la infraestructura tecnológica y las tarifas HyperLedger (blockchain recomendada), sino que también contemple la capacitación del director TI en tecnología blockchain, asegurando que el equipo de TI tenga las competencias necesarias para la implementación exitosa.

2. Inicio de la Prueba de Concepto

Se recomienda a la Dirección de TI y el Departamento de Desarrollo de Software comenzar con una prueba de concepto en el mediano plazo (3-6 meses).

La prueba de concepto debe centrarse en un caso de uso limitado, como la emisión de certificados para un programa piloto o un grupo de egresados específico (del Centro de Especialización Universitario CEU), lo cual permitirá validar la viabilidad técnica en un entorno controlado.

Este paso es permitirá probar la integración real del Módulo de Emisión con el Sistema de Gestión de Procesos existente de la universidad y para medir el desempeño, la escalabilidad y los costos operativos de la blockchain seleccionada (HyperLedger) antes de una implementación a gran escala. La experiencia piloto servirá para afinar el diseño arquitectónico y mitigar riesgos futuros.

3. Integración del Módulo de Emisión y la Interfaz de Validación QR

El Departamento de Desarrollo de Software, bajo el liderazgo del Director de TI, debe priorizar la integración funcional y completa de los componentes diseñados en el mediano plazo (6-12 meses).

Esto implica desarrollar el Módulo de Emisión en Blockchain para generar el hash de los nuevos certificados de forma automática y garantizar su registro inmutable, resolviendo así de raíz los puntos de vulnerabilidad identificados en el diagnóstico.

Paralelamente, es necesario desarrollar la Interfaz de Validación con QR que será la herramienta principal de terceros, asegurando que el proceso de verificación sea instantáneo, amigable con el usuario y que cumpla con las expectativas de eficiencia y rapidez demandadas por las empresas encuestadas.

4. Creación e Implementación del Protocolo de Seguridad y Privacidad

La Dirección de TI tiene la responsabilidad de establecer formalmente el Protocolo de Protección de Datos en el corto plazo (0-6 meses). Este protocolo debe detallar rigurosamente cómo se realizará la *hashización (transformación de datos en hashes)* de los datos, el método de gestión y custodia de las claves privadas de la universidad (para firmar transacciones) y la forma en que el sistema

garantiza la privacidad de la información personal, limitando la *blockchain* a registrar únicamente la huella digital del documento.

El cumplimiento estricto de la normativa de protección de datos es una condición indispensable para lograr la Aceptación Externa del sistema y minimizar los riesgos legales y reputacionales.

5. Capacitación al Personal Clave

El Departamento de TI debe diseñar e implementar un plan de capacitación exhaustivo en el mediano plazo (3-6 meses). Este plan debe centrarse no solo en los nuevos procedimientos operativos de emisión y gestión, sino también en proveer una comprensión fundamental de la tecnología Blockchain a las autoridades académicas y al personal administrativo.

Abordar la variable de Percepción del Personal a través de la formación disminuirá la resistencia al cambio, incrementará la confianza en el sistema y asegurará la correcta ejecución del nuevo Proceso de Emisión de Certificados, logrando que el personal se convierta en promotor interno de la innovación.

6. Comunicación Externa y Estrategia de Adopción

Finalmente, la Dirección de Mercadeo y la Rectoría deben ejecutar una estrategia de comunicación proactiva en el largo plazo (12+ meses), una vez que el sistema piloto esté estable y operativo.

Esta estrategia debe ir dirigida específicamente a los empleadores, instituciones de educación superior y organismos reguladores, promocionando la implementación del sistema blockchain como una ventaja competitiva de la universidad en términos de seguridad, transparencia y agilidad.

Este esfuerzo capitalizará la alta Necesidad de Validación de Terceros identificada, fortaleciendo la reputación de la UISIL como una institución innovadora y comprometida con la autenticidad y seguridad de las credenciales de sus egresados.

BIBLIOGRAFÍA

Blockchain para Micro-credenciales: más allá de la Firma Digital. (22 de abril de 2025). Obtenido de Acreditta: https://info.acreditta.com/blog/credenciales-digitales/blockchain-para-micro-credenciales-mas-alla-firma-digital/

Bartolome Pina, A., Bellver Torla, C., Castañeda Quintero, L., & Adell, S. J. (2017). *Blockchain en Educación: introducción y crítica al estado de la cuestión. Edutec, Revista Electrónica De Tecnología Educativa, (61), a363.* Obtenido de doi.org: https://doi.org/10.21556/edutec.2017.61.915

Blockchain en la Universidad. (8 de Junio de 2020). Obtenido de CRUE: https://www.crue.org/wp-content/uploads/2022/03/Blockhain-en-la-universidad_TIC-360_FINAL_BAJA.pdf

Ventajas del Blockchain en Educación. (s.f.). Obtenido de IEP: https://www.iep-edu.com.co/5-ventajas-del-blockchain-en-educacion/

Blockchain en la educación: su uso en credenciales académicas. (2022). Obtenido de Universidad Nacional Autónoma de México.: https://www.revista.unam.mx/2022v23n1/blockchain_en_la_educacion_su_uso_en_credenciales_academicas/

Beneficios de la tecnología Blockchain en educación. (s.f.). Obtenido de uPlanner: https://uplanner.com/es/tecnologia-blockchain-educacion/

Sharma, V., & Gupta, A. (2024). Development of Blockchain-Based Academic Credential Verification System. *Scientific Research Publishing.*

Patel, M., Soni, M., & Vaghela, S. (2023). mplementing Blockchain Based Credentials In Education Sector In India. *Frontiers in Health Informatics.*

Musa, I., Ibrahim, M., & Abdullahi, M. (2024). Certificate Validation Using Blockchain. *ResearchGate.*

Taylor, & Francis. (2025). Enhancing Educational Certificate Management and Verification with Blockchain Technology. *Taylor & Francis Online.*

Al-Ma'ani, M., El-Telbany, O., & Al-Qatawneh, L. (2024). Utilizing Blockchain Technology for University Certificate Verification System. *International Journal of Computer Applications.*

Nakamoto, S. (s.f.). *Bitcoin: A peer-to-peer electronic cash system.* Obtenido de https://bitcoin.org/bitcoin.pdf

Garcia-Bañuelos, L., Ponomarev, D., & Dumas, M. (2019). Blockchain y su aplicación en sistemas descentralizados. *Revista Iberoamericana de Informática Educativa, *12*(1), 45-60.*, 45-60.

UCenfotec. (2023). *¿Qué es el blockchain? Una explicación simple.* Obtenido de https://ucenfotec.ac.cr/que-es-el-blockchain-una-explicacion-simple/

AcademiaBID. (s.f.). *Credenciales Digitales.* Obtenido de https://cursos.iadb.org/es/programas/credenciales-digitales

AEBanca. (s.f.). *DLT (Blockchain). Asociación Española de Banca.* Obtenido de https://s1.aebanca.es/wp-content/uploads/2017/10/DLT-Blockchain.pdf

Amo Filvà, D. (2020). Privacidad, seguridad y legalidad en soluciones educativas basadas en Blockchain: Una Revisión Sistemática de la Literatura. RIED. *Revista Iberoamericana de Educación a Distancia,*, 23(1), 221-235.

ANCYPEL. (2024). *Blockchain revoluciona la verificación de credenciales académicas.* . Obtenido de ANCYPEL: https://www.ancypel.es/index.php/actualidad/noticias/1810-blockchain-revoluciona-la-verificacion-de-credenciales-academicas

SHA256, el algoritmo de Bitcoin. (2023). Obtenido de Bit2Me Academy: https://academy.bit2me.com/sha256-algoritmo-bitcoin/

Aplicaciones del Blockchain en el Mundo Real. (2024). Obtenido de Bitstamp: https://www.bitstamp.net/es/learn/crypto-101/real-world-applications-of-blockchain/

Blockchain en Educación: Cadenas rompiendo moldes. (2018). Obtenido de Fundación Aula Smart. : https://www.lmi-cat.net/sites/default/files/10_blockchain.pdf

Qué es blockchain y para qué sirve. (s.f.). Obtenido de Grant Thornton: https://www.grantthornton.es/insights/articulos/que-es-blockchain/

¿Qué es un contrato inteligente? (2022). Obtenido de IBM: https://www.ibm.com/mx-es/topics/smart-contracts

Un ejemplo de educación financiada mediante criptomoneda: la ICO de la IEBS Business School. (2020). Obtenido de IEBSchool: https://www.tecnologia-ciencia-educacion.com/index.php/TCE/article/view/375

Preukschat, A. (2017). *Blockchain: La revolución industrial de internet.* Ediciones Gestión 2000. Obtenido de Preukschat.

¿Qué es la tokenización? (2025). Obtenido de Signeblock: https://www.signeblock.com/es/que-es-la-tokenizacion

¿Qué son las credenciales digitales? . (s.f.). Obtenido de Thomas Signe.: https://www.thomassigne.com/es-es/productos-y-soluciones/credenciales-digitales

Hayes, A. (s.f.). *Datos sobre blockchain: qué es, cómo funciona y cómo se puede utilizar*. Obtenido de Investopedia: https://www.investopedia.com/terms/b/blockchain.asp

AWS. (s.f.). *¿Qué es la descentralización en la cadena de bloques?* Obtenido de AWS: https://aws.amazon.com/es/web3/decentralization-in-blockchain/

Chen, Y., Pereira, I., & Lee, J. (2021). Blockchain in education: Preventing credential fraud. *Journal of Educational Technology Systems*, *49*(3), 345–362.

Solana vs Ethereum. (s.f.). Obtenido de TabTrader: https://tabtrader.com/es/academy/articles/solana-vs-ethereum-is-solana-really-an-ethereum-killer

Computer, H. (s.f.). *1,3 millones por un NFT: cada vez más famosos se unen al club de los monos*. Obtenido de Computer Hoy: https://computerhoy.20minutos.es/noticias/tecnologia/13-millones-nft-cada-vez-famosos-unen-club-monos-1006115

AWS. (2024). *¿Qué es la criptografía?* Obtenido de Amazon Web Services: https://aws.amazon.com/es/what-is/cryptography/

Acreditta. (s.f.). *6 formas de reducir el fraude académico en Universidades.* Obtenido de Acreditta: https://info.acreditta.com/blog/educacion/formas-reducir-fraude-academico/

Rios-Avendaño, C., Ocampo-Salazar, C., & Nuñez, M.-A. (2024). Gestión del riesgo de fraude académico en educación superior. Un análisis en universidades de

Medellín, Colombia, en tiempos de COVID-19. *Revista Iberoamericana de Educación Superior*.

Dias-Barriga, A., & Hernandez Rojas, G. (2002). *Estrategias docentes para un aprendizaje significativo: Una interpretación constructivista. .* McGraw-Hill Interamericana.

Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, P. (2014). *etodología de la investigación (6ta ed.).* McGraw-Hill Education.

Kerlinger, F., & Lee, H. (2002). *Investigación del comportamiento (4ta ed.).* McGraw-Hill.

Montero, L., & León, M. (2007). *Investigación educativa: Un enfoque cualitativo y cuantitativo. .* Editorial C.C.S.

Bernal, C. A. (2010). *Metodología de la investigación (3ra ed.).* Bogotá, Colombia: Pearson Educación.

ANEXOS

Anexo 1. Cuestionario para Autoridades Académicas: Verificación de Certificados Académicos

Cuestionario para Autoridades Académicas: Verificación de Certificados Académicos

Estimado(a) funcionario administrativo(a) de UISIL:

Le saluda Ing. Guillermo Mora Granados, Director de Tecnología de Información (TI) de la Universidad Internacional San Isidro Labrador (UISIL).

Actualmente, me encuentro liderando una investigación fundamental para el futuro de la educación superior y la seguridad en la contratación: la **"Propuesta de la arquitectura tecnológica para un sistema de validación de Certificados Académicos basado en Blockchain"**. Este proyecto tiene como meta el diseño e implementación de una solución tecnológica avanzada en la UISIL para prevenir el fraude en certificados y optimizar la verificación de credenciales de nuestros egresados.

Su rol como funcionario administrativo es de suma importancia para el éxito de esta iniciativa. Comprender su visión sobre la emisión y validación de certificados y el nivel de interés en tecnologías disruptivas como Blockchain nos permitirá diseñar un sistema que no solo beneficie a la UISIL, sino que también le brinde confianza a nuestros egresados y sus empleadores.

Le invitamos a dedicar aproximadamente 4 minutos de su tiempo para completar este breve cuestionario. Su colaboración es un aporte invaluable que asegura que la solución tecnológica se ajuste a las necesidades reales del mercado laboral.

Sus respuestas serán tratadas de forma **confidencial** y utilizadas exclusivamente con fines de investigación.

¡Muchas gracias por su valioso tiempo y apoyo a este proyecto de innovación!

Atentamente,

Ing. Guillermo Mora Granados
Director de Tecnologías de Información (TI)
Universidad Internacional San Isidro Labrador

* Indica que la pregunta es obligatoria

El objetivo de este cuestionario es recopilar la perspectiva de las altas autoridades sobre la problemática actual del fraude académico y la viabilidad, tanto estratégica como financiera, de implementar un sistema de validación de certificados basado en la tecnología Blockchain.

Sección 1. Identificación del participante

1. ¿Cuál es el cargo que desempeña en la Universidad? *
   - Rector
   - Gerente administrativo
   - Directora de registro
   - Director de CEU
   - Coordinadora de CEU

Sección 2. Bloque estratégico y BlockChain

2. ¿Cuál es su nivel de conocimiento actual sobre la tecnología BlockChain?*
   - Nulo conocimiento
   - Conocimiento básico
   - Conocimiento intermedio
   - Conocimiento bueno
   - Conocimiento avanzado/experto

Definición: Blockchain es una tecnología de registro digital distribuido que funciona como un libro de contabilidad compartido, donde la información se agrupa en bloques inmutables y se protege mediante criptografía. Su principal fortaleza reside en la inmutabilidad y la descentralización: una vez que un certificado se registra en la cadena, es prácticamente imposible de falsificar o alterar, y al estar distribuido en una red, la autenticidad se puede verificar de forma instantánea y sin necesidad de intermediarios, ofreciendo una solución de ciberseguridad robusta contra el fraude académico.

3. ¿En qué medida considera que la adopción de Blockchain en la certificación posicionaría a la UISIL como una institución líder en innovación tecnológica?*
   - Mínimo (en total desacuerdo)
   - En desacuerdo
   - Neutral (impacto moderado)
   - De acuerdo
   - Totalmente de acuerdo

4. Además de certificados y títulos, ¿en qué otras áreas ve potencial para aplicar la tecnología Blockchain en la universidad?*
   - Registro inmutable de notas o calificaciones.
   - Gestión de contratos o archivos sensibles.
   - Procesos de votaciones estudiantiles.

- Control de inventario.
- No veo potencial en otras áreas por ahora.
- Otros:

Sección 3: Fraude con certificados falsos

5. ¿Cuál es su nivel de preocupación respecto al riesgo actual o potencial de fraude (falsificación/alteración) con certificados académicos?*

- 1 (Mínimo): Muy Baja preocupación
- 2: Baja preocupación
- 3: Preocupación Moderada
- 4: Alta preocupación
- 5 (Máximo): Máxima preocupación

6. ¿Qué tan eficiente y rápida considera que es la Universidad en la verificación de certificados ante solicitudes de terceros (ej. empleadores o instituciones educativas externas)?*

- 1 (Mínimo): Nada eficiente (Proceso lento y manual)
- 2: Poco eficiente
- 3: Aceptable
- 4: Eficiente
- 5 (Máximo): Muy eficiente (Proceso automatizado y rápido)

7. ¿Cuál cree que es el principal impacto que el fraude académico tiene o podría tener sobre la institución?*

- Daño Reputacional y pérdida de prestigio.
- Riesgo Legal y posibles sanciones.
- Costos Económicos por gestión de fraude y validaciones manuales.
- Debilitamiento de la Confianza en la calidad educativa.
- Todos los anteriores en similar medida.

8. Según su criterio, mencione la característica más importante que debe tener un nuevo sistema de validación para combatir drásticamente el fraude y mejorar la confianza.*

_____

Sección 4: Aspecto Presupuestario y Financiero

9. Considerando las prioridades institucionales, ¿qué nivel de prioridad asignaría a la asignación de un presupuesto para este proyecto de ciberseguridad basado en Blockchain?*

- (Mínimo): Baja prioridad
- Prioridad Modesta
- Prioridad Media (Debe ser considerado)
- Alta prioridad
- 5 (Máximo): Máxima prioridad (Debe ser presupuestado y ejecutado este año)

10. ¿Estaría su departamento dispuesto a evaluar una inversión inicial que prometa reducir costos a largo plazo (trámites manuales, litigios) y mitigar el riesgo de fraude? *

- Sí, Definitivamente.
- Sí, pero la inversión debe ser mínima.
- Depende de un Retorno de la Inversión (ROI) detallado y documentado.
- No, actualmente no es una prioridad de inversión.
- No, lo consideramos inviable financieramente.

11. ¿De qué partidas presupuestarias o fuentes se podrían obtener fondos para cubrir los costos de desarrollo, implementación y mantenimiento del sistema?*

- Partida de Inversión en Tecnología y Sistemas (TI).
- Fondo de Ciberseguridad / Riesgo Institucional.
- Reasignación del Presupuesto Operativo Anual.
- Fondos de Proyectos Especiales o Extensión.
- Se puede trasladar el costo a los estudiantes.

Sección 5: Aspectos Operacionales y Logísticos

12. ¿Cuál será el principal desafío u obstáculo operativo que enfrentará su área (Registro o CEU) con la implementación de este nuevo sistema de certificación?*

_____

13. ¿Qué medidas sugeriría para asegurar la aceptación y el uso de estos certificados digitales por parte de empleadores, gobiernos y otras instituciones externas? *

_____

Anexo 2. Cuestionario para Empleadores: Verificación de Certificados Académicos

Cuestionario para Empleadores: Verificación de Certificados Académicos

Estimado(a) empleador(a):

Le saluda Ing. Guillermo Mora Granados, Director de Tecnología de Información (TI) de la Universidad Internacional San Isidro Labrador (UISIL).

Actualmente, me encuentro liderando una investigación fundamental para el futuro de la educación superior y la seguridad en la contratación: la **"Propuesta de la arquitectura tecnológica para un sistema de validación de Certificados Académicos basado en Blockchain"**. Este proyecto tiene como meta el diseño e implementación de una solución tecnológica avanzada en la UISIL para prevenir el fraude en certificados y optimizar la verificación de credenciales de nuestros egresados.

Su experiencia como empleador es de suma importancia para el éxito de esta iniciativa. Comprender los desafíos que enfrenta su empresa al validar títulos, la frecuencia del fraude percibido y el nivel de interés en tecnologías disruptivas como Blockchain nos permitirá diseñar un sistema que no solo beneficie a la UISIL, sino que también sirva como una herramienta de seguridad y eficiencia para su proceso de selección.

Le invitamos a dedicar aproximadamente 4 minutos de su tiempo para completar este breve cuestionario. Su colaboración es un aporte invaluable que asegura que la solución tecnológica se ajuste a las necesidades reales del mercado laboral.

Sus respuestas serán tratadas de forma **confidencial, anonimizadas** y utilizadas exclusivamente con fines de investigación.

¡Muchas gracias por su valioso tiempo y apoyo a este proyecto de innovación!

Atentamente,

Ing. Guillermo Mora Granados
Director de Tecnologías de Información (TI)
Universidad Internacional San Isidro Labrador

* Indica que la pregunta es obligatoria

Objetivo: Recolectar información sobre la experiencia actual de las empresas en la validación de credenciales académicas y evaluar el interés y la viabilidad de implementar un sistema de verificación instantáneo y seguro basado en tecnología Blockchain para los certificados emitidos por la Universidad Internacional San Isidro Labrador.

Su nombre completo:

_____

Nombre de la empresa que representa:

_____

Sección I: Fraude en Certificados y Proceso de Verificación Actual

Esta sección busca identificar la frecuencia y los desafíos del proceso de verificación de credenciales en su organización.

1. ¿Con qué frecuencia su empresa verifica los certificados, títulos o diplomas de los postulantes o empleados?*

- Siempre o en el 100% de los casos.
- Frecuentemente (50% - 99% de los casos).
- Ocasionalmente (1% - 49% de los casos).
- Rara vez o nunca.

2. En una escala del 1 al 5, ¿qué tan importante considera el proceso de verificación de certificados académicos para su proceso de contratación? (Siendo 1: Nada importante y 5: Crítico)*

- 1
- 2
- 3
- 4
- 5

3. ¿Ha detectado o sospechado de certificados académicos fraudulentos (falsificados o alterados) en los últimos 3 años?*

- Sí, hemos detectado casos de fraude.
- Sí, hemos tenido sospechas, pero no se ha confirmado.
- No, nunca hemos detectado o sospechado de fraude.

4. Cuando realiza una verificación con una institución educativa, ¿cuál es el tiempo promedio de respuesta que experimenta?*

- Menos de 24 horas.
- De 1 a 3 días hábiles.
- De 4 días a 1 semana.
- Más de 1 semana.

5. ¿Cuál de los siguientes es el principal problema que enfrenta su empresa al verificar certificados académicos? (Seleccione solo uno) *

- Alto riesgo de fraude/falsificación (dudas sobre la autenticidad).
- Demoras en la respuesta de las instituciones.
- Alto costo administrativo/tiempo invertido por el personal de RR.HH.
- Falta de un proceso estandarizado y claro.

Sección II: Interés en un Sistema de Validación Digital

Esta sección evalúa el valor percibido de un sistema de validación moderna para optimizar sus procesos.

6. Si existiera un sistema que le permitiera verificar la autenticidad de un certificado de forma instantánea y en línea (24/7), ¿qué tan interesado estaría en utilizarlo?*

- Muy interesado, lo implementaría de inmediato.
- Interesado, lo consideraría seriamente.
- Neutral.
- Poco interesado.
- Nada interesado.

7. ¿Cuál es el atributo más valioso que buscaría en un nuevo sistema de validación de certificados? (Seleccione solo uno) *

- Confiabilidad/Seguridad (Garantía de que el certificado no es fraudulento).
- Rapidez/Inmediatez de la verificación.
- Facilidad de uso (Pocos pasos para la verificación).
- Acceso a información detallada sobre el logro académico (calificaciones, plan de estudios).

8. ¿Cree que la facilidad y rapidez en la verificación de credenciales académicas impactaría positivamente en la eficiencia de sus procesos de contratación?*

- Sí, de forma muy significativa.
- Sí, moderadamente.
- No estoy seguro/a.
- No, tendría poco o ningún impacto.

Sección III: Conocimiento y Aceptación de Blockchain

Esta sección explora la familiaridad con la tecnología Blockchain y su aceptación para la gestión de credenciales.

9. ¿Qué tanto conocimiento tiene sobre la tecnología Blockchain (Cadena de Bloques)?*

- Tengo un conocimiento profundo (Entiendo su funcionamiento y aplicaciones).
- Tengo un conocimiento básico (Conozco el concepto general de descentralización e inmutabilidad).
- Conozco el nombre, pero no sé cómo funciona.
- No tengo conocimiento alguno.

10. La tecnología Blockchain garantiza la inmutabilidad (un registro no puede ser alterado) y la descentralización de los datos. ¿Qué tan valiosas son estas características para la verificación de un certificado académico?*

- Extremadamente valiosas (Son la solución al fraude).
- Muy valiosas.
- Algo valiosas.
- Poco valiosas.
- No son valiosas.

11. Suponiendo que un sistema de validación basado en Blockchain cumple con todas las leyes de protección de datos, ¿su empresa estaría dispuesta a utilizar este tipo de tecnología para la verificación de certificados?*

- Definitivamente sí.
- Probablemente sí.
- No estoy seguro/a.
- Probablemente no.
- Definitivamente no.

Anexo 3. Propuesta de un Sistema de Emisión y Validación de Certificados en BlockChain.

MAESTRÍA EN CIBERSEGURIDAD

Propuesta de la arquitectura tecnológica para un sistema de validación de Certificados Académicos basado en Blockchain para la prevención del fraude en la Universidad Internacional San Isidro Labrador durante el periodo lectivo 2025

AUTOR
Ing. Guillermo Mora Granados

Pérez Zeledón, Costa Rica
Diciembre, 2025

PROPUESTA RECOMENDADA DEL PROCESO DE EMISIÓN Y VALIDACIÓN.

La arquitectura propuesta se compone de tres capas principales y una infraestructura de soporte.

Capa 1: Capa de Interfaz y Emisión

Esta capa se basa en la infraestructura interna de la UISIL.

- **Sistema de Gestión de Procesos (SGP):** El sistema actual utilizado por el CEU para generar el certificado digital (PDF).
- **Módulo de Integración Blockchain:** El nuevo módulo propuesto. Su función es recibir el certificado digital (PDF) del SGP, generar su huella digital criptográfica (hash) y firmarlo digitalmente con la clave privada de la UISIL.

Capa 2: Capa de Lógica y Automatización (*Smart Contracts*)

Esta capa reside directamente en la red Blockchain Ethereum.

- **Contrato Inteligente de Certificación:** El programa central que gestiona la lógica de emisión. Está programado para aceptar únicamente transacciones de registro de hash firmadas con la clave pública de la UISIL. Al recibir el hash y la firma, lo registra en el libro de contabilidad distribuido (Blockchain).
- **Registro Inmutable (Ledger):** El libro de contabilidad donde se almacenan permanentemente: el hash del certificado, la fecha y hora de emisión y la identificación única del certificado (ID de la transacción o token ID. Importante: Solo se almacena el hash, no los datos personales del estudiante lo que garantiza que la información personal del estudiante no se publica en la red de Blockchain.

Capa 3: Capa de Verificación y Acceso (Terceros)

Esta capa es accesible públicamente para los verificadores (empleadores, instituciones).

- **Módulo de Validación Web:** Una interfaz de usuario simple y optimizada para la consulta, con estrictos protocolos de protección de datos. Es la plataforma a la que se redirige al escanear el código QR.
- **Herramienta de Hashing Local:** Un componente dentro del Módulo de Validación que, al subir un certificado PDF, calcula su hash de forma local en el navegador del usuario.

PROCESO DETALLADO DE EMISIÓN

Figura 1. Flujo simplificado del proceso de emisión de certificados.

Nota: Elaboración propia.

PROCESO DETALLADO DE VERIFICACIÓN

El proceso de verificación es instantáneo y sin intermediarios.

1. **Solicitud de Verificación:** Un empleador escanea el **Código QR** impreso o digital en el certificado del estudiante.
2. **Redirección al MVW:** El QR redirige al empleador al **Módulo de Validación Web (MVW)** e introduce automáticamente el ID de la transacción.
3. **Carga del Certificado:** Se le solicita al empleador que suba el archivo PDF del certificado que desea verificar.

4. **Cálculo de Hash Local:** La **Herramienta de Hashing Local** en el MVW calcula el hash criptográfico del PDF subido por el empleador (Hash A).
5. **Consulta a la Blockchain:** El MVW consulta la red Blockchain utilizando el ID de la transacción (obtenido del QR) para recuperar el hash registrado por la UISIL (Hash B).
6. **Comparación Instantánea:** El sistema compara **Hash A** (del documento cargado) con **Hash B** (del registro inmutable de la Blockchain).
7. **Resultado:**
    - **Si Hash A = Hash B:** El certificado es **AUTÉNTICO**. La inmutabilidad del registro garantiza que el documento no ha sido alterado desde su emisión oficial.
    - **Si Hash A ≠ Hash B:** El certificado es **NO AUTÉNTICO** (Falsificado o Alterado). El intento de manipulación ha cambiado el hash del documento, rompiendo la coincidencia.

SELECCIÓN JUSTIFICADA DE LA PLATAFORMA BLOCKCHAIN

El estudio de viabilidad técnica (Objetivo Específico 2) debe decantarse por una plataforma que equilibre **seguridad/inmutabilidad** (propia de redes públicas) con **control/costo/escalabilidad** (esenciales para un proyecto institucional).

Tabla 1. Tabla comparativa entre las dos plaformas disponibles para la emisión de certificados.

Criterio	Ethereum (pública)	Hyperledger Fabric
Tipo de Red	Permissionless	Permissioned
Permissioned: para la emisión; el control es clave para la emisión oficial.		
Inmutabilidad	Alta (Descentralización Global)	Alta (Descentralización entre Nodos del Consorcio)
Alta. Ambas son fuertes, pero la inmutabilidad de la emisión se garantiza con el hash en el ledger.		
Costo (Gas)	Muy Alto y Variable 8080	Cero a Bajo (tasas internas)
Bajo a Cero. La UISIL necesita una solución de bajo costo operativo para la emisión masiva.		
Escalabilidad	Limitada (depende de Capa 2)	Alta (Diseñada para Empresa/Consorcio)
Alta. Necesaria para el volumen de certificados anuales.		
Protección de datos.	Requiere diseño complejo (almacenar solo Hash)	Más fácil de implementar (datos fuera de la cadena en nodos controlados)
Diseño de Hash Only. Cumplimiento legal es primordial.		

Nota: Elaboración propia

RECOMENDACIÓN ARQUITECTÓNICA (JUSTIFICACIÓN):

Se propone una solución de **Blockchain de Consorcio (*Permissioned*)** utilizando la plataforma **Hyperledger Fabric o Besu** (si se desea compatibilidad con la EVM, Ethereum Virtual Machine) o bien, un **Contrato Inteligente en una Red Pública de Bajo Costo y Alta Escalabilidad (ej. Solana)**.

- **Opción A (Recomendada): Hyperledger Fabric.** Proporciona el control, la baja latencia y el bajo costo operativo que necesita la UISIL, permitiendo gestionar una red con sus socios (otras universidades, empleadores clave) como nodos verificadores.
- **Opción B (Alternativa): Solana o Polygon (L2 de Ethereum).** Si la prioridad es la máxima descentralización y la verificación *global*, se usaría una red pública de alta velocidad/bajo costo (Solana) o una Capa 2 (Polygon) para mitigar el costo del gas, manteniendo el sistema de Smart Contract (CIC) que solo acepta la clave privada de la UISIL para registrar el hash.

El diseño del **Módulo de Integración Blockchain (MIA-B)** debe ser independiente de la plataforma, preparado para interactuar mediante una API con el *Smart Contract* o el *Chaincode* de la red elegida, lo que garantiza la flexibilidad del sistema