Propuesta de Arquitectura Tecnológica para un Sistema de Certificación Académica Basado en Blockchain para la Prevención del Fraude

Ing. Guillermo Mora Granados
Universidad Internacional San Isidro Labrador (UISIL)
guillermo.mora@uisil.ac.cr

Resumen

Los sistemas tradicionales de emisión y validación de certificados académicos en la Universidad Internacional San Isidro Labrador (UISIL) enfrentan una alta vulnerabilidad al fraude, ineficiencia operativa y falta de control por parte de los estudiantes. Esta investigación propone un diseño arquitectónico tecnológico para un sistema de validación de certificados académicos utilizando la tecnología Blockchain. La solución se centra en aprovechar las propiedades de inmutabilidad y descentralización de la cadena de bloques para anclar la huella digital criptográfica (hash) de cada certificado, garantizando su autenticidad y previniendo la falsificación. El proyecto diagnostica la situación actual, realiza un estudio de viabilidad técnica y compara plataformas blockchain para diseñar un módulo que integre los certificados con una red de bloques, permitiendo la verificación instantánea mediante códigos QR y empoderando al estudiante con el control de sus credenciales. La implementación de esta arquitectura posicionará a la UISIL a la vanguardia tecnológica, blindará la integridad académica y reducirá los costos administrativos asociados a la verificación manual

Palabras Clave

Blockchain, Smart Contract, Criptografía, Descentralización, Inmutabilidad, Certificados académicos, Validación de certificados, Prevención de fraude, Autenticidad, Transparencia, Hashing, Arquitectura tecnológica

Abstract

Traditional systems for issuing and validating academic certificates at the Universidad Internacional San Isidro Labrador (UISIL) face high vulnerability to fraud, operational inefficiency, and lack of student control. This research proposes a technological architectural design for an academic certificate validation system using Blockchain technology. The solution focuses on leveraging the properties of immutability and decentralization of the blockchain to anchor the cryptographic digital fingerprint (hash) of each certificate, guaranteeing its authenticity and preventing counterfeiting. The project diagnoses the current situation, conducts a technical feasibility study, and compares blockchain platforms to design a module that integrates the certificates with a block network, enabling instant verification using QR codes and empowering the student with control over their credentials. Implementing this architecture will position UISIL at the technological forefront, shield academic integrity, and reduce administrative costs associated with manual verification.

Keywords
Blockchain, Smart Contract, Cryptography, Decentralization, Immutability, Academic certificates, Certificate validation, Fraud prevention, Authenticity, Transparency, Hashing, Technological architecture.

I. INTRODUCCIÓN

La gestión de credenciales académicas es una función esencial y crítica en cualquier institución de educación superior. Sin embargo, los métodos convencionales basados en documentos físicos y procesos manuales han demostrado ser insuficientes frente a las crecientes amenazas de ciberseguridad y la demanda de eficiencia en la era digital.

II. PLANTEAMIENTO DEL PROBLEMA

La Universidad Internacional San Isidro Labrador (UISIL) opera actualmente con un sistema de emisión de

certificados que presenta tres problemas críticos interrelacionados:

1. **Vulnerabilidad al Fraude y la Falsificación:** La dependencia de formatos físicos o digitales sin un sistema robusto de validación facilita la manipulación de calificaciones, la creación de certificados fraudulentos y la suplantación de identida. Esta debilidad compromete directamente el prestigio de la institución y la confianza en sus egresados. Los autores Al-Ma'ani et al. (2024) y Bapat (2020) han señalado que esta vulnerabilidad es una debilidad intrínseca de los sistemas tradicionales.
2. **Ineficiencia Operativa y Carga Administrativa:** La emisión de documentos requiere procesos manuales (impresión, sellado, firma) y logística para el retiro físico, generando altos costos y demoras. La verificación de la autenticidad por parte de terceros (empleadores o instituciones externas) es un proceso lento y dependiente de la comunicación directa con la universidad.
3. **Falta de Control del Estudiante:** Los estudiantes carecen de un control directo y eficiente sobre sus documentos académicos, que son susceptibles a pérdida o daño, y cuya compartición con terceros es manual y lenta.

III. JUSTIFICACIÓN Y BENEFICIOS ESTRATÉGICOS

La adopción de una solución basada en Blockchain es un paso estratégico que alinea a la UISIL con su visión de ser una entidad proactiva y a la vanguardia tecnológica. La tecnología de cadena de bloques ofrece un registro inmutable, seguro y transparente, eliminando la posibilidad de falsificación y la dependencia de intermediarios. La importancia de este proyecto se centra en sus múltiples beneficiarios:

- **La Universidad:** Fortalece la imagen institucional, reduce procesos manuales y optimiza la eficiencia en la emisión y verificación de certificados.
- **Los Estudiantes:** Obtienen control total sobre sus credenciales pudiendo compartirlas de forma segura e instantánea con terceros, facilitando su inserción laboral.
- **Empleadores y Otras Instituciones:** Se benefician de un sistema de verificación instantánea y confiable, agilizando procesos de contratación y selección, e incrementando la confianza en las credenciales de los egresados de la UISIL.

IV. OBJETIVOS DEL PROYECTO

El proyecto se limita a la fase de **definición y planificación**, estableciendo las bases conceptuales para una implementación futura.

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.

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.

V. FUNDAMENTOS DE LA TECNOLOGÍA BLOCKCHAIN

La Blockchain es un tipo de Libro de Contabilidad Distribuido (DLT) que registra transacciones de forma segura, secuencial y permanente en bloques enlazados criptográficamente. Se diferencia de las bases de datos típicas en que almacena datos en bloques vinculados mediante criptografía, lo que garantiza su **inmutabilidad** y **descentralización**.

VI. DESCENTRALIZACIÓN, DISTRIBUCIÓN E INMUTABILIDAD

La **descentralización** implica la transferencia del control de una entidad centralizada (como una universidad tradicional) a una red distribuida de participantes. En la Blockchain, múltiples nodos conservan una copia del registro completo, eliminando el "punto único de falla" y la necesidad de confiar en un intermediario.

La **inmutabilidad** es la propiedad de que un dato, una vez registrado en la cadena de bloques, no puede ser modificado ni eliminado. Se logra mediante:

- **Estructura de Bloques Encadenados:** Cada bloque contiene el **hash** (firma digital) del bloque anterior, creando una dependencia cronológica.
- **Funciones Hash Criptográficas:** Algoritmos (como SHA-256) que generan identificadores únicos e irreversibles para cada conjunto de datos. Si se altera un bloque, su hash cambia abruptamente, rompiendo la cadena y alertando a la red, lo que garantiza la integridad académica y elimina la posibilidad de falsificación.

VII. HASH Y FIRMAS CRIPTOGRÁFICAS

El **hash** es el pilar de la seguridad en la blockchain. Es una sucesión alfanumérica de longitud fija, producida por una **función hash** (algoritmo matemático), que identifica de manera inequívoca un documento o conjunto de datos. Las características clave son:

- **Unicidad:** Dos entradas diferentes nunca generarán dos hash idénticos.
- **Irreversibilidad (Unidireccionalidad):** A partir del hash, no se puede descifrar el dato de entrada original, lo que es fundamental para la seguridad.

En el sistema de certificación, el hash del certificado digital actúa como su huella digital criptográfica inalterable.

VIII. CONTRATOS INTELIGENTES (*SMART CONTRACTS*)

Los **Contratos Inteligentes** son programas informáticos que se almacenan y ejecutan automáticamente en la blockchain cuando se cumplen condiciones predefinidas. Estos programas "autoejecutables" eliminan la necesidad de intermediarios humanos, ya que el propio código garantiza el cumplimiento de los términos.

En la certificación, un *Smart Contract* podría activarse al detectar el cumplimiento de los requisitos de graduación de un estudiante. Una vez activado, automáticamente genera el certificado digital y ancla su hash a la blockchain, firmándolo con la clave de la universidad. Esto agiliza el flujo de trabajo, previene errores humanos y reduce costos administrativos.

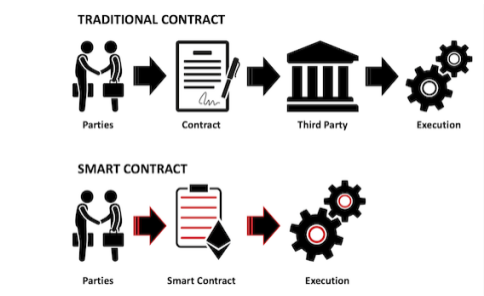


Figura 1. Comparativa entre contratos tradicionales vs contratos inteligentes.

IX. APLICACIÓN EN EL ÁMBITO EDUCATIVO

La tecnología Blockchain ofrece una solución transformadora a los problemas de las credenciales académicas.

De Credenciales Físicas a Digitales Seguras

Los certificados físicos, validados con sellos y firmas, son vulnerables a la pérdida, deterioro y falsificación, y su verificación es un proceso manual y burocrático.

Las **Credenciales Digitales** basadas en blockchain, en cambio, son un paquete de datos seguro, verificable en línea y estandarizad. Incluyen metadatos detallados (emisor, receptor, criterios cumplidos) y, al estar ancladas en la blockchain, son intrínsecamente portátiles y seguras.

Verificación de Credenciales Automatizada

La verificación tradicional es un cuello de botella, dependiente de la comunicación directa con la institución. La Blockchain automatiza este proceso: la universidad registra el hash del certificado en la cadena, y cualquier tercero puede verificar instantáneamente la autenticidad comparando el hash del documento con el registro inalterable de la blockchain. La coincidencia del hash demuestra la autenticidad al instante, eliminando intermediarios y acortando los tiempos de verificación, lo que es un beneficio directo para los empleadores.

Identidad Digital Soberana (SSI)

La SSI permite a los individuos ser los custodios de su propia identidad y registros, sin depender de autoridades centrales. En el ámbito educativo, un certificado basado en blockchain permite al estudiante almacenar la credencial en su cartera digital y decidir selectivamente qué información compartir, cuándo y con quién. Esto aumenta la autonomía, protege la privacidad y agiliza los procesos, siendo un avance fundamental en la confianza del ecosistema educativo.

X. MARCO METODOLÓGICO

El proyecto se enmarca en una **investigación descriptiva** de enfoque mixto (cualitativo y cuantitativo) con un diseño de **propuesta de arquitectura**.

XI. TIPO Y ABORDAJE DE LA INVESTIGACIÓN

El objetivo principal no es la implementación, sino el **diseño**. Por lo tanto, el trabajo se basa en el **Diagnóstico** de la situación actual y la **Propuesta de Diseño Arquitectónico**.

- **Finalidad:** Aplicada, orientada a resolver el problema del fraude de certificados en la UISIL.
- **Abordaje:** Se sigue una metodología estructurada en fases, similar a un enfoque de Design Science Research (DSR), que busca crear un artefacto (la propuesta de arquitectura) para resolver un problema de gestión.

XII. SUJETOS Y FUENTES DE INFORMACIÓN

Se utilizan fuentes primarias para obtener la información necesaria para el diseño.

- **Sujetos de Información (Población y Muestreo):**
  - **Autoridades Académicas y Funcionarios Clave:** Personal del Centro de Extensión Universitaria (CEU) y Registro, quienes manejan los procesos de emisión de certificados. Se aplica una entrevista a profundidad para diagnosticar el proceso actual, obstáculos y riesgos.
  - **Empleadores y Empresas (Terceros Verificadores):** Muestra de empresas que contratan egresados de la UISIL (posibles empleadores). Se aplica una encuesta para cuantificar la frecuencia de verificación, la importancia del proceso, el tiempo de respuesta experimentado con el sistema actual, la incidencia de fraude detectado y el interés en un sistema basado en Blockchain.

XIII. INSTRUMENTOS PARA RECOLECCIÓN Y ANÁLISIS DE DATOS

Los instrumentos se diseñan para cubrir los objetivos de diagnóstico y viabilidad.

- **Entrevista a Autoridades Académicas (Cualitativa):** Se busca mapear el proceso actual, identificar vulnerabilidades, evaluar el nivel de conocimiento sobre Blockchain, y anticipar desafíos u obstáculos operativos en la implementación del nuevo sistema.
- **Encuesta a Empresas/Empleadores (Cuantitativa):** Mide la percepción sobre la importancia de la verificación, la eficiencia del sistema actual de la universidad y el nivel de aceptación de la tecnología Blockchain para la verificación instantánea. Los resultados de esta encuesta se utilizan para justificar la necesidad

del sistema y priorizar sus atributos clave

XIV. ESTUDIO DE VIABILIDAD TÉCNICA Y COMPARATIVA DE PLATAFORMAS

Se investigan plataformas como **Ethereum**, **Solana** y **Hyperledger**, y se genera una matriz de análisis comparativo. La selección debe justificarse en función de criterios clave para el contexto universitario:

- **Costo de Transacción (Gas):** Plataformas como Ethereum (pública) pueden tener costos considerablemente altos, lo que es una restricción y riesgo identificado en el proyecto. Esto puede llevar a considerar una solución de Capa 2 (Layer 2) o una plataforma con tarifas más bajas (como Solana) o una red privada/consorcio (como Hyperledger Fabric o Besu).
- **Tipo de Red:**
  - **Pública (Permissionless):** Mayor descentralización e inmutabilidad, pero menor control y altos costos/baja escalabilidad (ej. Ethereum, Solana).
  - **Privada/Consorcio (Permissioned):** Mayor control sobre los participantes, mejores tasas de transacción y menor latencia (ej. Hyperledger Fabric). Dado que la UISIL necesita controlar quién emite los certificados, una red *permissioned* o un contrato inteligente en una red pública que limite la emisión a una clave autorizada (la de la UISIL) es esencial.
- **Escalabilidad y Rendimiento:** Capacidad para manejar el volumen esperado de emisión de certificados y solicitudes de verificación sin latencia.
- **Cumplimiento Normativo (Protección de Datos):** La arquitectura debe garantizar que la información personal sensible (nombre, calificaciones) no se almacene directamente en la cadena de bloques pública, sino que solo se ancle el hash, cumpliendo con las leyes de protección de datos[69].

XV. PROPUESTA DE ARQUITECTURA TECNOLÓGICA PARA LA VALIDACIÓN DE CERTIFICADOS

El diseño arquitectónico propuesto se centra en complementar el Sistema de Gestión de Procesos existente en la UISIL (que emite certificados digitales) con un nuevo módulo que integre esta emisión con una red Blockchain para garantizar la inmutabilidad y autenticidad[717171].

XVI. ARQUITECTURA CONCEPTUAL DEL SISTEMA

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.

XVII. PROCESO DETALLADO DE EMISIÓN



Figura 2. Flujo simplificado del proceso de emisión de certificados.

XVIII. 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.

XIX. 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).

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.		

Tabla1. Tabla comparativa entre las dos plaformas disponibles para la emisión de certificados.

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.

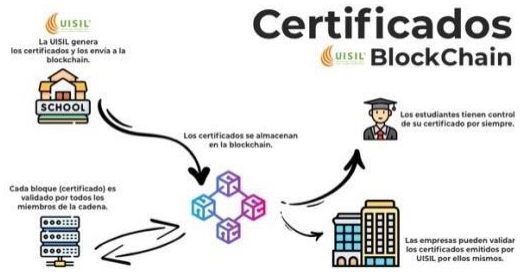


Ilustración 1. Proceso propuesto de emisión y validación de certificados académicos.

XX. CONCLUSIONES

El desarrollo de la propuesta arquitectónica ha permitido alcanzar los objetivos planteados:

1. **Diagnóstico de Vulnerabilidad:** Se ha confirmado que la arquitectura tecnológica actual de la UISIL, dependiente de procesos manuales y documentos físicos/digitales sin validación robusta, es altamente susceptible al fraude y genera ineficiencia operativa, socavando la credibilidad institucional y demorando los procesos de terceros.
2. **Viabilidad y Selección de Plataforma:** El estudio de viabilidad técnica ha demostrado que la tecnología Blockchain (DLT) es viable para resolver el problema del fraude de certificados. El análisis comparativo subraya que una arquitectura basada en un sistema *Permissioned* (Hyperledger Fabric) o una solución de Capa 2/Red de Bajo Costo (Solana/Polygon) en una red pública es la opción más adecuada, priorizando el control institucional y la mitigación de los costos de transacción masivos (gas).
3. **Diseño Arquitectónico Robusto:** Se ha diseñado una arquitectura de tres capas (Emisión, Lógica, Verificación) que utiliza la función de hashing para anclar la huella digital del certificado a la cadena de bloques y un Smart Contract para automatizar el proceso de registro. Este diseño garantiza la inmutabilidad del registro, permite la verificación instantánea mediante códigos QR y cumple con los protocolos de protección de datos al almacenar únicamente el hash, no la información personal.

XXI. RECOMENDACIONES

Basado en la propuesta de diseño, se recomienda a la Universidad Internacional San Isidro Labrador:

1. **Continuar con la Fase de Desarrollo (Prototipo y Piloto):** Asignar el presupuesto necesario para la siguiente etapa, que es la implementación de un prototipo funcional del Módulo de Integración Blockchain (MIA-B) y el Módulo de Validación Web (MVW).
2. **Inversión y Presupuesto:** Evaluar la inversión inicial que, aunque significativa, promete una reducción de costos a largo plazo (eliminación de trámites manuales, litigios, fraude). Es necesario determinar las partidas presupuestarias para cubrir los costos de desarrollo, implementación y mantenimiento del sistema.
3. **Integración de Datos y *Smart Contracts*:** Comenzar la planificación detallada para la integración del nuevo sistema con el SGP existente, y desarrollar el Contrato Inteligente de Certificación (CIC). Se debe definir con precisión la lógica de negocio que activará la emisión automática, asegurando que solo los registros académicos validados por el CEU puedan generar el hash en la Blockchain.
4. **Marco Legal de Privacidad de Datos:** El protocolo de protección de datos debe asegurar el cumplimiento total de la legislación nacional e internacional, especialmente en lo relativo a la gestión de información personal sensible, garantizando que la inmutabilidad de la cadena de bloques se aplique únicamente al hash y no a la identidad del estudiante.

XXII. REFERENCIAS

[1] G. Mora Granados, "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," Maestría en Ciberseguridad, Universidad Internacional San Isidro Labrador, Pérez Zeledón, Costa Rica, 2025.

[2] Al-Ma'ani, A. et al., "Blockchain-Based Academic Certificate Verification System: A Systematic Review," Journal of Cybersecurity and Information Security, 2024.

[3] A. Bapat, "Blockchain Technology in Educational Record Keeping," International Journal of Computer Applications, 2020.

[4] S. Sharma y P. Gupta, "Leveraging Blockchain for Fraud Reduction in Academic Certifications," International Conference on Information Technology, 2024, p. 2.

[5] A. Al-Ma'ani et al., "Blockchain and Smart Contracts for Automated Certificate Verification," International Journal of Computer Applications, 2024.

[6] P. Patel, "Immutable Records and Trust in Blockchain Credentials," Journal of Educational Technology Systems, vol. 51, no. 1, p. 2, 2023.

[7] M. Musa et al., "Efficacy of Blockchain in Securing Academic Records: A Case Study," Journal of Computing and Information Technology, vol. 32, no. 1, p. 5, 2024.

[8] Taylor & Francis, "Decentralization for Enhanced Transparency and Security in Academic Verification," Academic Press, p. 1, 2025.

[9] Grant Thornton, "¿Qué es Blockchain?," Grant Thornton (s.f.).

[10] S. Preukschat, Blockchain: La revolución industrial de Internet, 2.ª ed. ed. España: Gestión 2000, 2017.

[11] Bit2Me Academy, "Qué es un hash," Bit2Me Academy (2023).

[12] AWS, "¿Qué es la descentralización en la cadena de bloques?," Amazon Web Services (AWS) (s.f.).

[13] IBM, "Contratos inteligentes," IBM (2022).

[14] Bitstamp, "Inmutabilidad de la Blockchain," Bitstamp (2024).

[15] X. Chen et al., "Blockchain-Based System for Academic Certificates: Design and Implementation," IEEE Access, vol. 9, 2021.

[16] AcademiaBID, "Credenciales digitales," AcademiaBID (s.f.).

[17] ANCYPEL, "Blockchain y el fin de la falsificación documental," ANCYPEL (2024).

[18] Fundación Aula Smart, "Blockchain en la educación," Fundación Aula Smart (2018).

[19] A. Amo Filvà, "Identidad Digital Soberana (SSI): Un nuevo paradigma," Revista de Ciberseguridad y Privacidad, 2020.