Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), septiembre-octubre 2026,
Volumen 10, Número 5.

https://doi.org/10.37811/cl_rcm.v10i5

EL MECANISMO BLOCKCHAIN DE VERIFICACIÓN APLICADO EN CERTIFICADOS ACADÉMICOS Y DE PARTICIPACIÓN: UNA REVISIÓN BIBLIOGRÁFICA

THE BLOCKCHAIN VERIFICATION MECHANISM APPLIED TO ACADEMIC AND PARTICIPATION CERTIFICATES: A LITERATURE REVIEW

Rodrigo Sthefano Benítez Miranda
Universidad Estatal Amazónica, Ecuador

David Sancho Aguilera
Universidad Estatal Amazónica, Ecuador

DOI: https://doi.org/10.37811/cl_rcm.v10i5.26446

El Mecanismo Blockchain de Verificación Aplicado en Certificados Académicos y de Participación: Una Revisión Bibliográfica

Rodrigo Sthefano Benítez Miranda[1]
rs.benitezm@uea.edu.ec
https://orcid.org/0000-0002-9743-3069
Universidad Estatal Amazónica
Ecuador

David Sancho Aguilera
dsancho@uea.edu.ec
https://orcid.org/0000-0001-5625-4198
Universidad Estatal Amazónica
Ecuador

RESUMEN

La verificación de la autenticidad de los certificados académicos y de participación constituye un problema persistente para la educación superior. Este trabajo presenta una revisión bibliográfica sistemática sobre la aplicación de la tecnología de cadena de bloques a dicha verificación, con el objetivo de establecer el grado de madurez alcanzado por las soluciones documentadas y derivar una propuesta aplicable a la Universidad Estatal Amazónica. A partir de 81 registros identificados se conformó, mediante un procedimiento de depuración en seis pasos y la verificación de cada referencia contra su fuente primaria, un corpus final de 39 trabajos publicados entre 2019 y 2026. Los resultados muestran un campo en expansión antes que en consolidación: de los 28 sistemas documentados, 26 no superan el estadio de prototipo y uno solo alcanza producción real verificada. El análisis identifica además un desajuste entre el modelo de amenaza de esta literatura, que presupone un emisor no confiable, y la configuración habitual del caso institucional, donde el emisor constituye la parte confiable y los riesgos se localizan en la alteración posterior del documento y en la fabricación de ejemplares nunca emitidos. De ello se deriva un modelo de adopción organizado en cuatro fases.

Palabras clave: cadena de bloques, verificación de credenciales, certificados académicos, integridad documental, educación superior

[1] Autor principal
Correspondencia: rs.benitezm@uea.edu.ec

The Blockchain Verification Mechanism Applied to Academic and Participation Certificates: A Literature Review

ABSTRACT

Verifying the authenticity of academic and participation certificates remains a persistent problem for higher education. This paper presents a systematic literature review on the application of blockchain technology to such verification, aiming to establish the maturity actually reached by documented solutions and to derive a proposal applicable to Universidad Estatal Amazónica. From 81 identified records, a final corpus of 39 works published between 2019 and 2026 was assembled through a six-step screening procedure and the verification of every reference against its primary source. Results show a field in expansion rather than consolidation: of the 28 documented systems, 26 do not exceed the prototype stage and only one reaches verified production deployment. The analysis further identifies a mismatch between the threat model underlying this literature, which presupposes an untrusted issuer, and the usual configuration of the institutional case, where the issuer is the trusted party and risks lie in post-issuance alteration and in the fabrication of never-issued copies. A four-phase adoption model is derived from this finding.

***Keywords*:** blockchain, credential verification, academic certificates, document integrity, higher education

Artículo recibido 13 setiembre 2026
Aceptado para publicación: 20 octubre 2026

INTRODUCCIÓN

La falsificación de credenciales académicas constituye un fenómeno de alcance económico considerable y documentado. Castro y Au-Yong-Oliveira (2021), sobre datos del National Student Clearinghouse, sitúan el mercado global de credenciales falsificadas en torno a los dos mil millones de dólares, con ejemplares comercializados entre 350 y 4.000 dólares por unidad. Las encuestas sobre conducta declarativa en procesos de selección arrojan cifras convergentes: Awaji et al. (2020), sobre datos de Higher Education Degree Datacheck y de NGA HR Services, reportan que aproximadamente el 30 % de los estudiantes y titulados ha exagerado sus logros académicos, que el 90 % de los directores de recursos humanos ha detectado exageraciones en las postulaciones recibidas y que un 32 % de los postulantes falsea específicamente sus cualificaciones educativas. El costo que ello impone a una organización promedio se estima en hasta 40.000 libras esterlinas anuales.

El problema no se agota, sin embargo, en la falsificación deliberada. La verificación de credenciales legítimas conlleva a su vez una fricción considerable: Castro y Au-Yong-Oliveira (2021) documentan que el reconocimiento de un título brasileño en Portugal puede requerir hasta 500 euros y entre tres y seis meses de trámite, en un procedimiento que involucra traducciones juradas y legalizaciones consulares. Verificar resulta costoso tanto cuando el documento es falso como cuando es auténtico.

La severidad con que este problema se manifiesta no se distribuye de manera uniforme. Las descripciones más contundentes proceden de contextos donde la verificación continúa siendo un procedimiento manual. El-Dorry et al. (2020) señalan que en Egipto la obtención de un certificado falso se ha vuelto común, al punto de permitir a quien lo porta postular a un empleo y ser considerado tan calificado como quien posee uno legítimo. Farabi et al. (2025) sitúan el fraude de credenciales como una amenaza a la integridad educativa, especialmente en países en desarrollo como Bangladesh, donde los métodos de verificación son principalmente manuales e ineficientes.

La transición hacia la emisión digital de documentos ha modificado los términos del problema sin resolverlo. Un certificado distribuido en formato electrónico resulta más fácil de obtener y de transmitir, pero también más fácil de modificar, y su verificación sigue dependiendo en la mayoría de los casos de que quien lo recibe confíe en la apariencia del documento o consulte directamente a la institución emisora. La disponibilidad de un archivo no equivale a la comprobación de su integridad.

Frente a esta situación, la literatura técnica ha propuesto durante la última década el recurso a la tecnología de cadena de bloques, cuya propiedad de inmutabilidad permitiría registrar la emisión de un certificado de modo que cualquier alteración posterior resultara detectable sin necesidad de recurrir al emisor. La producción académica sobre esta aplicación se ha intensificado de forma marcada a partir de 2023. Determinar si esa intensificación se corresponde con una madurez tecnológica equivalente constituye una condición previa para cualquier decisión institucional fundada al respecto, y es precisamente la cuestión que este trabajo se propone establecer.

En el ámbito latinoamericano, la incorporación de estas tecnologías presenta un desarrollo desigual. Guerschberg y Gutiérrez (2025) documentan experiencias en Argentina, Perú, Ecuador y Colombia, y advierten que las profundas desigualdades estructurales en el acceso a tecnologías, la fragmentación de los sistemas educativos y la escasa interoperabilidad entre instituciones universitarias han generado un terreno fértil para la exploración de soluciones descentralizadas. El informe del Observatorio Iberoamericano de la Ciencia, la Tecnología y la Sociedad (Organización de Estados Iberoamericanos, 2026) coincide en que la adopción regional aún enfrenta desafíos vinculados con la infraestructura digital, la regulación y la formación de capacidades especializadas.

El caso que motiva este trabajo se sitúa en ese contexto. La Universidad Estatal Amazónica emite certificados de participación editorial a autores y revisores por su intervención en cada número o edición de sus publicaciones periódicas. Estos documentos se acompañan de un código que enlaza al archivo alojado en el servidor institucional, mecanismo que resuelve la localización del documento pero no acredita su integridad: permite encontrar el certificado, no comprobar que el ejemplar en poder de un tercero coincide con el emitido.

La decisión de emprender una revisión bibliográfica con anterioridad a cualquier desarrollo responde a un criterio deliberado: definir la estrategia de adopción a partir de fundamentación teórica y de la experiencia documentada por instituciones que enfrentan un caso equivalente, en lugar de derivarla de supuestos propios. A ello se suma una consideración de orden institucional: un proceso sustentado en evidencia publicada resulta más apto para convocar a otras entidades a participar de forma colaborativa, en la medida en que ofrece a los eventuales aliados una base verificable sobre la cual evaluar su propia incorporación.

El objetivo general de este trabajo es ofrecer al lector institucional un mapa del estado real de la cuestión, con indicación del grado de madurez efectivamente alcanzado por las soluciones documentadas. El propósito no es persuadir respecto de su adopción, sino permitir que cada institución determine con prontitud si la línea se ajusta a su propia realidad, y que esa determinación, afirmativa o negativa, se apoye en el antecedente bibliográfico que la sustenta.

Terminología básica

Blockchain. Caramihai y Severin (2023) definen la tecnología de cadena de bloques como una red de igual a igual compuesta por libros de registro descentralizados y distribuidos, en la que las transacciones quedan marcadas con fecha y hora y almacenadas de forma consensuada entre las partes, lo que hace prácticamente imposible alterarlas o cometer fraude sin ser detectado. Bajo este esquema, un certificado emitido queda como prueba inmutable, verificable por administradores y empleadores con el permiso del titular.

Función hash criptográfica. Berrios Moya et al. (2025) explican el mecanismo que hace posible la verificación de integridad documental: cada archivo se identifica mediante un hash criptográfico único en lugar de un nombre de archivo; si el archivo es modificado, su hash cambia, lo que hace que cualquier alteración sea detectable de inmediato. Esta propiedad constituye la base técnica de toda propuesta de verificación que no dependa únicamente de la confianza en el servidor que aloja el archivo.

Contrato inteligente. Fartitchou et al. (2025) señalan que plataformas como Ethereum permiten el desarrollo de contratos inteligentes autoejecutables, que automatizan y hacen cumplir acuerdos sin necesidad de intermediarios. En el contexto de la certificación académica, un contrato inteligente puede automatizar el registro del hash de un certificado en el momento de su emisión, sin intervención manual posterior.

Certificado de participación editorial. En el contexto institucional de este estudio, se entiende por tal el documento que la Universidad Estatal Amazónica emite a autores y revisores por su intervención en un número o edición de sus publicaciones periódicas, como constancia formal de su rol en el proceso editorial.

METODOLOGÍA

El presente estudio adopta el enfoque de revisión bibliográfica sistemática empleado por Cherrafi et al. (2016) para la integración de sistemas de gestión, adaptado a la búsqueda de literatura sobre cadena de bloques aplicada a la verificación de certificados académicos y de participación. Se trata de un estudio de tipo documental y alcance descriptivo, con diseño transversal. A diferencia de una revisión con protocolo fijado a priori, el proceso de selección se documenta aquí en sus tres etapas reales, porque cada una incorporó un criterio o sesgo académico explícito que conviene declarar, no ocultar, siguiendo el principio de trazabilidad que exige toda revisión sistemática rigurosa.

El presente estudio adopta el enfoque de revisión bibliográfica sistemática empleado por Cherrafi et al. (2016) para la integración de sistemas de gestión, adaptado a la búsqueda de literatura sobre cadena de bloques aplicada a la verificación de certificados académicos y de participación. Se trata de un estudio de tipo documental y alcance descriptivo, con diseño transversal. A diferencia de una revisión con protocolo fijado a priori, el proceso de selección se documenta aquí en sus tres etapas reales, porque cada una incorporó un criterio o sesgo académico explícito que conviene declarar, no ocultar, siguiendo el principio de trazabilidad que exige toda revisión sistemática rigurosa.

Identificación

La búsqueda se realizó mediante herramientas de descubrimiento asistidas por inteligencia artificial, Perplexity y la función de investigación web de NotebookLM, en dos rondas: una búsqueda amplia sobre cadena de bloques y verificación de certificados académicos, acotada al período 2019-2026, y una segunda búsqueda dirigida a reforzar la representación de países latinoamericanos distintos de Ecuador, dado que la primera arrojó un corpus concentrado en producción técnica internacional con escasa presencia regional. Este proceso identificó 81 registros de tipos heterogéneos: artículos de revista, actas de congreso, tesis, preprints, informes institucionales y portales oficiales.

Depuración progresiva

Sobre los 81 registros identificados se aplicó, de forma iterativa, un criterio cada vez más exigente sobre qué constituye evidencia citable en una revisión bibliográfica formal. La Tabla 1 resume el resultado del proceso y la Tabla 2 detalla el criterio aplicado en cada paso, con la razón académica que lo sustenta.

Tabla 1. Embudo de selección del corpus

Etapa del proceso de selección	Excluidos	Restantes
Registros identificados en las dos rondas de búsqueda	—	81
Exclusión de tesis de grado y maestría no arbitradas	16	65
Verificación de indexación real, referencia por referencia	10	55
Exclusión de fuentes no académicas	4	51
Exclusión de informes institucionales aislados	6	45
Exclusión de portales de alcance nacional único	2	43
Exclusión tras la lectura y verificación del texto completo	4	39

Fuente: elaboración propia.

Tabla 2. Criterios de exclusión aplicados en cada paso

Paso	Criterio aplicado	Sesgo o razón académica	Excl.	Rest.
1	Excluir tesis de grado y maestría no arbitradas	Una tesis no ha pasado por revisión por pares; se reserva como evidencia contextual, no como literatura arbitrada	16	65
2	Priorizar por tipo e indexación real, verificada y no asumida	Se verificó una por una la indexación (Scopus, Web of Science, SciELO, Latindex); varias revistas resultaron sin confirmación o con señales de baja selectividad editorial	10	55
3	Excluir fuentes no académicas y de confianza no verificable	Blogs corporativos, portales de producto comercial y referencias citadas solo de forma secundaria no constituyen evidencia académica	4	51
4	Excluir informes institucionales aislados	Un informe sin respaldo de un organismo intergubernamental o de alcance regional aporta un caso anecdótico, no evidencia generalizable	6	45
5	Excluir portales oficiales sin alcance multinacional	Se conservó únicamente el portal con mayor valor evidencial para la propuesta aplicada: una red ya operativa entre países	2	43
6	Excluir, tras la lectura del texto completo, lo no existente, no verificable o ajeno al objeto de estudio	Solo posible después de leer las fuentes: una referencia trataba de gestión genérica de datos personales; otra resultó inaccesible; una tercera no correspondía a ningún documento real; una cuarta carecía de datos de publicación verificables	4	39

Fuente: elaboración propia.

Un criterio explícito guio esta depuración y merece señalarse porque corrige un sesgo intuitivo: las actas de congreso arbitradas (ACM Digital Library; series Springer LNCS, LNNS y CCIS) se conservaron en su totalidad, mientras que varios artículos de revista fueron excluidos por indexación no confirmada.

Esto responde a que, en ciencias de la computación, un acta de congreso arbitrada puede representar mayor rigor metodológico que un artículo publicado en una revista de bajo estándar editorial: descartar por *tipo* de publicación en lugar de por *calidad* verificada habría introducido un sesgo de selección contrario al propósito de la revisión.

Verificación fuente por fuente

Antes de dar el corpus por cerrado se verificó cada referencia contra su documento original, leyendo el texto completo cuando el acceso lo permitió y, en caso contrario, contrastando los metadatos con al menos dos bases independientes (CrossRef, DBLP, Semantic Scholar y OpenAlex). Esta verificación reveló que 22 de las 43 referencias que entonces integraban el corpus contenían algún error de citación: autorías incompletas o invertidas, años de publicación incorrectos, títulos truncados, revistas mal atribuidas y, en dos casos, identificadores digitales que remitían a artículos distintos de los citados, con otro título y otro equipo de autores. La totalidad de estos errores fue corregida contra la fuente primaria. La verificación llevó además a excluir cuatro registros adicionales por las razones consignadas en el paso 6 de la Tabla 2, con lo que el proceso resultó en un corpus final de 39 registros: 22 artículos de revista, 12 actas de congreso arbitradas, 3 preprints académicos y 2 fuentes institucionales de alcance regional, retenidas de forma deliberada por su valor evidencial para la propuesta aplicada. La proporción de errores encontrada desaconseja construir una revisión bibliográfica a partir de metadatos de segunda mano; uno de ellos resultó, de hecho, heredado de una fuente del propio corpus, que atribuía a un autor una afiliación nacional que no le corresponde.

Limitaciones del estudio

Cuatro limitaciones condicionan el alcance de los resultados. La primera, y de mayor peso metodológico, es que el cribado y la clasificación del corpus fueron realizados por un único revisor; las revisiones sistemáticas recomiendan la participación de al menos dos revisores independientes en las fases de selección y extracción, precisamente para acotar el sesgo individual en la aplicación de los criterios. La documentación detallada del procedimiento busca compensar parcialmente esta limitación mediante la trazabilidad de cada decisión, pero no la sustituye.

La segunda concierne al grado de acceso efectivo a las fuentes: de las 39 referencias, 16 pudieron consultarse en texto completo o en extensión suficiente, 13 únicamente a través de su resumen y 9 solo

mediante metadatos bibliográficos verificados, debido a las restricciones de acceso de IEEE Xplore, Springer Nature y ACM Digital Library. La clasificación por enfoque técnico y grado de madurez resulta, en consecuencia, más robusta para el primer grupo.

La tercera se refiere al procedimiento de búsqueda: la identificación inicial se apoyó en herramientas asistidas por inteligencia artificial, cuyo comportamiento de recuperación no es enteramente reproducible ni auditable del mismo modo que una ecuación de búsqueda ejecutada sobre una base de datos bibliográfica, por lo que no puede descartarse la omisión de trabajos pertinentes. La cuarta atañe a la cobertura: la búsqueda se circunscribió a producción en español e inglés publicada entre 2019 y 2026.

RESULTADOS Y DISCUSIÓN

Caracterización bibliométrica del corpus

La producción sobre cadena de bloques aplicada a la verificación de certificados académicos resulta incipiente hasta 2022 y se acelera de forma marcada a partir de 2023, según muestra la Tabla 3. El año 2025 concentra por sí solo la mayor producción individual, lo que sugiere que el campo se encuentra en una fase de expansión activa antes que consolidada.

Tabla 3. Distribución del corpus por año de publicación

Año	2019	2020	2021	2022	2023	2024	2025	2026
N.º de referencias	2	7	3	5	6	3	11	2

Fuente: elaboración propia.

El corpus reúne producción de 23 países o agrupaciones regionales. India concentra la mayor proporción individual, con 7 referencias, seguida de Portugal y Grecia con 3 cada uno. La dispersión resultante indica que la preocupación por esta cuestión no está circunscrita a un polo geográfico único. En cuanto al idioma, el 87,2 % del corpus está publicado en inglés y el 12,8 % en español, y estas últimas coinciden exactamente con las fuentes de alcance regional y local retenidas, lo que confirma que el idioma de publicación se correlaciona con la proximidad geográfica del fenómeno estudiado.

Siguiendo el criterio de delimitación mundial, regional y local, el corpus se concentra de forma abrumadora en el nivel macro, con 34 referencias (87,2 %). El nivel meso latinoamericano reúne 3 referencias (7,7 %) y el nivel micro ecuatoriano únicamente 2 (5,1 %), ninguna de las cuales supera el estadio de la simulación o del modelo conceptual.

Líneas de investigación identificadas

La clasificación por enfoque técnico permite distinguir dos grupos de tamaño desigual: 28 trabajos proponen un sistema de verificación, mientras que 11 corresponden a revisiones, estudios de adopción o informes de contexto. La Tabla 4 desagrega el conjunto.

Tabla 4. Distribución del corpus por enfoque técnico predominante

Enfoque técnico predominante	N.º	%
Arquitectura híbrida (huella en cadena, documento fuera de ella)	10	25,6
Cadena pública con contratos inteligentes	7	17,9
Cadena permisionada o de consorcio	5	12,8
Red interinstitucional o multicadena	2	5,1
Privacidad avanzada (pruebas de conocimiento cero)	1	2,6
Sistema propuesto sin especificar la cadena	3	7,7
Revisiones y estudios bibliométricos	9	23,1
Estudio de adopción o percepción	1	2,6
Informe institucional de contexto	1	2,6
Total	**39**	**100**

Fuente: elaboración propia.

La arquitectura híbrida constituye la línea dominante. Su predominio responde a una solución de compromiso adoptada de forma convergente por el campo: la cadena registra únicamente la huella criptográfica del documento, mientras que el archivo permanece en almacenamiento externo, habitualmente el sistema de archivos interplanetario, empleado de forma explícita en 8 de los 28 sistemas. Esta división obedece a dos restricciones simultáneas, el costo de almacenar documentos completos en cadena y la tensión entre la inmutabilidad del registro y la normativa de protección de datos personales. Resulta llamativo, en cambio, que la privacidad avanzada constituya el eje de diseño de un solo sistema, pese a que dicha tensión aparece señalada como limitación en varios de los trabajos restantes: el campo reconoce el problema con mayor frecuencia de la que lo aborda como objeto central de diseño.

Madurez de las soluciones reportadas

La clasificación de los 28 sistemas según su grado de desarrollo efectivo, presentada en la Tabla 5, arroja el hallazgo de mayor peso de esta revisión.

Tabla 5. Grado de madurez de los sistemas documentados

Grado de madurez alcanzado	N.º	% de 28
Propuesta conceptual o diseño, sin implementación	4	14,3
Prototipo implementado, sin evaluación reportada	11	39,3
Prototipo implementado y evaluado	10	35,7
Sistema en producción real	2	7,1
No determinable con el material accesible	1	3,6
Total	**28**	**100**

Fuente: elaboración propia.

Un solo sistema cuenta con producción real verificada de forma académica: la plataforma desarrollada por Maestre et al. (2022), cuyos autores declaran de manera expresa que el sistema se encuentra en producción en una escuela de negocios española, con 34 certificados emitidos en pruebas. El segundo caso clasificado en producción, el proyecto regional de RedCLARA (2024), se sustenta en la declaración institucional de la propia red y no en verificación académica independiente, matiz que conviene conservar al citarlo.

El contraste entre la abundancia de propuestas y la escasez de despliegues se confirma al examinar las trayectorias de investigación más sostenidas. Rustemi et al. publicaron en 2023 una revisión sistemática del campo y en 2024 la propuesta aplicada derivada de ella; esta última, sin embargo, declara de forma explícita que el proceso de implementación formará parte de un estudio posterior. El proyecto BlockAdemiC, con al menos tres publicaciones entre 2022 y 2025 procedentes de dos subequipos del mismo centro griego (Terzi et al., 2022; Tepelidis et al., 2023, 2025), alcanzó un estudio de factibilidad tecnológica con evaluación de rendimiento, pero sitúa el despliegue a gran escala en el terreno de lo que puede considerarse más adelante. La continuidad en la publicación no se traduce, en este campo, en continuidad hacia el despliegue.

Plataformas tecnológicas predominantes

Ethereum y las cadenas compatibles con su máquina virtual concentran el mayor número de implementaciones, con 10 de 28, seguidas de las plataformas Hyperledger, con 5 casos, y de las cadenas derivadas de EOS, con 2. La frecuencia, sin embargo, no coincide con el desempeño reportado ni con la evidencia de despliegue. El único estudio del corpus que compara plataformas bajo condiciones equivalentes (Dash et al., 2025) mide entre 150 y 280 transacciones por segundo en Hyperledger Fabric,

frente a 20-28 en Ethereum y 13-16 en Bitcoin para el mismo caso de uso, con latencias de entre 320 y 920 milisegundos según el número de participantes. A ello se suma un dato convergente: tanto el único sistema en producción verificada como la única red regional en operación emplean cadenas permisionadas. La literatura experimenta mayoritariamente sobre cadenas públicas, pero los dos casos que superaron el umbral del laboratorio no lo hicieron sobre ellas.

Barreras y limitaciones reportadas

Las limitaciones que los propios autores declaran configuran un patrón consistente, en el que las barreras de adopción pesan más que las dificultades técnicas. La primera es el costo de migración: Nadeem et al. (2023) advierten que el costo de trasladar el sistema existente a la cadena de bloques resulta extremadamente alto, lo que lo vuelve inviable para muchas organizaciones, y que la sustitución de los sistemas tradicionales por sistemas puramente basados en cadena resulta arriesgada, especialmente en países en desarrollo, en tanto requiere cambios sociales, legales y políticos mayores.

La segunda es la centralización residual. Vidal et al. (2020), pese a implementar un prototipo sobre un estándar consolidado, reconocen que los perfiles de la entidad emisora y las listas de revocación permanecen alojados en servidores universitarios: ni siquiera las soluciones que el campo considera completas eliminan por entero la dependencia del servidor institucional. La tercera es la tensión con la protección de datos personales, señalada por Maestre et al. (2022), Dash et al. (2025) y Gómez Vieites et al. (2025); estos últimos advierten que, aun empleando almacenamiento externo, las referencias o huellas pueden seguir considerándose datos personales.

La cuarta es la resistencia institucional, que Caramihai y Severin (2023) identifican mediante encuesta y entrevistas a expertos junto al costo y a la integración con los sistemas existentes. La quinta es el aislamiento institucional de las soluciones: Said et al. (2025) enuncian que las iniciativas existentes no ofrecen una solución integral al problema de la falsificación, en tanto se enfocan únicamente en un solo nivel educativo o en una sola institución. Hsu et al. (2022) señalan una carencia paralela en el plano de la confianza, al observar que la mayoría de los sistemas solo puede garantizar que el diploma es verdadero, pero no que quien lo porta sea el destinatario legítimo ni que el emisor sea reconocido por todos.

Cabe consignar, finalmente, una ausencia. Solo dos trabajos del corpus evalúan la dimensión humana de la adopción: Evangelista Andrade y Amate (2025) reportan una medición de usabilidad y Caramihai y Severin (2023) realizan un estudio de percepción. El resto mide consumo de gas, latencia y rendimiento. La viabilidad técnica de estas soluciones se encuentra considerablemente mejor documentada que su viabilidad institucional.

DISCUSIÓN

El desajuste entre el modelo de amenaza y el caso institucional

Los resultados anteriores permiten sostener que el campo se encuentra en una fase de proliferación de propuestas y no de consolidación de sistemas. El 93 % de los sistemas documentados no ha superado el estadio de prototipo, y la producción se acelera precisamente en los años más recientes, lo que sugiere expansión antes que madurez. Para una institución que evalúe incorporarse a esta línea, el dato relevante no es la abundancia de literatura disponible, sino la escasez de casos en operación sobre los cuales apoyarse.

La segunda observación concierne al modelo de amenaza sobre el que opera la literatura revisada. Rustemi et al. (2023) sintetizan el propósito compartido por el campo al señalar que la cadena de bloques permite emitir certificados digitales inalterables y volver los sistemas de verificación más rápidos, más confiables e independientes de la autoridad central. Esa independencia respecto de la autoridad central constituye el objetivo declarado de la mayor parte del corpus, y presupone un emisor cuya palabra no basta.

El caso institucional más frecuente, sin embargo, presenta la configuración inversa. En una institución de educación superior que emite certificados de participación, el emisor es precisamente la parte confiable; quienes no lo son se sitúan aguas abajo: el portador que puede alterar el documento tras recibirlo, o el tercero que fabrica y comercializa ejemplares que nunca fueron emitidos. Frente a esa configuración, un registro de huellas criptográficas bajo custodia de la institución emisora ofrece dos garantías distintas. Ante la alteración, prueba la integridad: la huella del documento presentado no coincide con la registrada y la modificación queda en evidencia. Ante la falsificación, opera como lista de referencia autorizada: la ausencia de registro no indica que el documento haya sido alterado, sino que la institución nunca lo emitió.

Ninguno de los 28 sistemas revisados contempla esta etapa. La literatura transita directamente desde el estado documental previo hasta el despliegue en cadena, sin considerar la verificación por huella bajo anclaje institucional como fase intermedia. Este trabajo sostiene que dicha omisión no constituye una elección técnicamente fundada, sino una consecuencia del modelo de amenaza adoptado: desde el supuesto de un emisor no confiable, una garantía custodiada por el propio emisor carece de valor y, por tanto, no se formula. Al optimizar para el caso adverso, el campo omite un paso que resolvería el caso frecuente a un costo marginal. Dos trabajos del corpus bordean esta observación sin enunciarla: Vidal et al. (2020) al admitir la centralización residual de las soluciones existentes, y Nadeem et al. (2023) al advertir sobre la inviabilidad de la migración inmediata en países en desarrollo.

Lo anterior no invalida el recurso a la cadena de bloques, sino que delimita aquello que efectivamente aporta. El anclaje distribuido responde a dos riesgos que el registro institucional no cubre. El primero es la permanencia: una verificación que depende del servidor de la institución emisora se extingue con él, riesgo que Vidal et al. (2020) formulan al advertir que un certificado puede quedar sujeto a la imposibilidad de verificación debido a la no disponibilidad de la entidad emisora. El segundo es la validez interinstitucional: mientras la garantía permanezca bajo custodia exclusiva del emisor, constituye una atestación de la institución sobre sí misma. La incorporación de validadores externos transforma esa afirmación en un respaldo concurrente de varias entidades, que es precisamente la arquitectura del único proyecto regional en operación, donde la institución emisora es validada por su red nacional de investigación y educación, y esta a su vez por la red regional. Cabe notar que esta configuración determina también la elección técnica: una cadena con validadores institucionales es, por definición, permisionada.

Corresponde señalar, por último, una observación sobre el marco comparativo de esta literatura. En los trabajos del corpus a los que fue posible acceder en texto completo, la comparación se establece frente a la verificación manual, los procedimientos de legalización internacional o los repositorios centralizados. La infraestructura de firma electrónica, alternativa efectivamente desplegada en países que cuentan con certificación digital nacional, entre ellos Ecuador, no aparece evaluada como opción en ninguno de ellos, pese a que varios emplean criptografía de clave pública como componente interno de sus arquitecturas.

La tercera observación se refiere a la pertinencia contextual de esta literatura. El corpus procede mayoritariamente de contextos donde la verificación de credenciales ya se encuentra automatizada, mientras que las descripciones más severas del problema provienen de países donde continúa siendo manual, según se expuso en la introducción. Ecuador comparte esas condiciones estructurales en mayor medida que las de los contextos europeos de los que procede la mayor parte del corpus. La presente revisión no identificó ningún sistema de verificación de credenciales efectivamente desplegado en una institución ecuatoriana: las dos referencias nacionales halladas corresponden a una simulación en entorno virtualizado (Morales-Morales et al., 2020) y a un modelo conceptual sin implementación (Quinde Paucar et al., 2025). Señalarlo no constituye una concesión, sino la condición misma que vuelve pertinente la propuesta que se desarrolla a continuación.

Modelo propuesto para la Universidad Estatal Amazónica

En la Universidad Estatal Amazónica, cada certificado de participación editorial se emite acompañado de un código que enlaza al archivo alojado en el servidor institucional, de acceso público. El mecanismo cumple una función real y no debe subestimarse: resuelve la localización del documento y evita que la verificación dependa de una solicitud administrativa. Su alcance, sin embargo, se detiene allí. El código conduce al archivo, pero no aporta evidencia de que el ejemplar que obra en poder de un tercero coincida con el que la institución emitió, ni permite distinguir un certificado auténtico de uno fabricado por fuera del proceso editorial. El punto de partida no es, por tanto, la sustitución del sistema actual, sino su extensión.

En la práctica, un certificado de participación lleva la firma del responsable del proceso de certificación. Fuera de la institución, sin embargo, ese nombre rara vez resulta significativo para quien recibe el documento. Un certificado cuya integridad puede verificarse de forma independiente traslada el sujeto de la garantía: ya no responde por el documento la persona que lo suscribió, sino la institución que lo emitió, y lo hace de manera pública y consultable desde cualquier lugar.

El modelo propuesto introduce una modificación de naturaleza conceptual antes que tecnológica: el código deja de resolver a un archivo y pasa a resolver a un registro de verificación, desde el cual se accede al archivo. La diferencia no es de implementación, pues un archivo no puede pronunciarse sobre su propia validez, mientras que un registro sí.

La Tabla 6 detalla los elementos que dicho registro expone y la función probatoria de cada uno.

Tabla 6. Elementos del registro de verificación y su función probatoria

Elemento del registro	Función probatoria
Estado: vigente, anulado o no consta	Establece si la institución reconoce el documento. El caso negativo enfrenta a la falsificación fabricada por fuera del proceso editorial
Huella criptográfica del documento	Permite a un tercero recalcular la huella sobre el ejemplar en su poder y contrastarla; toda modificación posterior queda en evidencia
Fecha y hora de registro	Acredita el momento en que la institución incorporó el documento a su registro
Unidad emisora y número de edición	Vincula el certificado a un número o edición determinado de las publicaciones institucionales
Rol acreditado	Precisa la condición certificada: autoría, revisión o participación en comité editorial

Fuente: elaboración propia.

Tres precisiones resultan necesarias. La primera concierne a la revocación: la inclusión del estado anulado no es accesoria, pues un registro que solo pueda afirmar y nunca desdecirse carece de utilidad operativa. Vidal et al. (2020) advierten precisamente que las listas de revocación permanecen alojadas en servidores institucionales incluso en las soluciones basadas en estándares consolidados. La segunda concierne al régimen de consulta: si los registros resultaran accesibles de forma secuencial o enumerable, la institución publicaría de hecho un directorio de todas las personas que han recibido certificados. Farabi et al. (2025) documentan esta consecuencia en su propio prototipo al reconocer que el diseño expone públicamente los metadatos del certificado una vez conocido el identificador; el registro debe ser consultable únicamente a partir del certificado en poder del interesado, y no navegable como listado.

La tercera concierne a la denominación del mecanismo temporal. La constancia de fecha y hora que produce el registro institucional no constituye un sellado de tiempo en el sentido técnico del término, que supone la intervención de una autoridad de sellado independiente conforme a la norma RFC 3161. Se trata de evidencia de custodia institucional, y conviene nombrarla de ese modo para no atribuirle una garantía que no posee. Cabe señalar, en relación con ello, una diferencia respecto de la infraestructura de firma electrónica: en un documento firmado electrónicamente la evidencia viaja incorporada al propio archivo, lo que permite su validación sin conexión, mientras que en el modelo aquí propuesto la evidencia reside en el registro institucional y su consulta requiere acceso a este.

Esta dependencia constituye precisamente la limitación que las fases siguientes vienen a resolver.

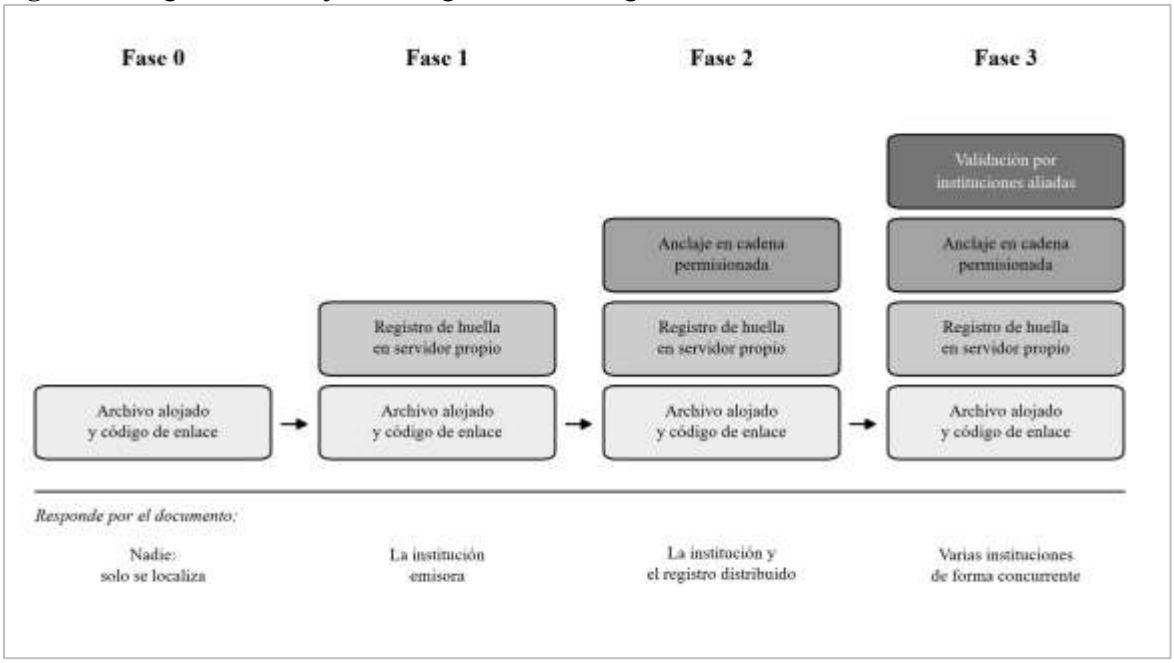
El modelo se organiza como una secuencia de fases en la que cada etapa responde a un riesgo distinto, según se detalla en la Tabla 7. Esta organización no obedece a consideraciones presupuestarias, sino a que los riesgos involucrados son de naturaleza diferente y admiten soluciones de alcance creciente.

Tabla 7. Ruta de adopción en cuatro fases

Fase	Mecanismo	Riesgo que atiende
0. Situación actual	Código enlazado al archivo alojado	Localización del documento
1. Registro institucional	Huella criptográfica, registro con metadatos y anclaje en servidor propio	Alteración del documento tras su recepción y fabricación de ejemplares no emitidos
2. Anclaje en cadena	Inscripción de huellas en cadena permisionada, con agrupación mediante árbol de Merkle	Extinción de la verificación junto con la infraestructura del emisor
3. Red interinstitucional	Validación concurrente por instituciones aliadas	Carácter auto-emitido de la garantía

Fuente: elaboración propia.

Figura 1. Progresión del sujeto de la garantía a lo largo de las cuatro fases



Fuente: elaboración propia.

La Fase 1 resuelve el riesgo efectivamente presente en el caso institucional. Su costo de implementación es marginal, en tanto no requiere infraestructura externa ni modificar el flujo editorial vigente, sino extender el mecanismo de publicación ya existente.

Su limitación debe declararse con la misma claridad: la garantía que produce descansa sobre la confianza en la institución emisora, que conserva la capacidad técnica de modificar tanto el documento como su registro.

La Fase 2 atiende un riesgo que la anterior no cubre, pues una verificación alojada en el servidor institucional se extingue con él: un cambio de dominio, una migración de infraestructura o la discontinuidad del servicio dejan sin medio de comprobación a certificados emitidos años atrás. La agrupación mediante árbol de Merkle, empleada por Vidal et al. (2020), permite que un único registro en cadena ampare un conjunto de certificados, lo que reduce el costo por documento a una fracción del que supondría el registro individual. La Fase 3 aborda la limitación que ninguna de las anteriores alcanza: mientras la garantía permanezca bajo custodia exclusiva del emisor, constituye una atestación de la institución respecto de sí misma, y la incorporación de validadores externos la transforma en un respaldo concurrente, especialmente pertinente cuando el certificado debe surtir efectos fuera del ámbito nacional.

La propuesta guarda con el corpus una relación de doble naturaleza: se apoya en él para las fases 2 y 3, y señala un vacío en la fase 1. La preferencia por una cadena permisionada se sustenta en tres elementos convergentes, ya expuestos: es la arquitectura del único sistema con producción real verificada, la del único proyecto regional en operación y la que registra el mejor desempeño en el único estudio comparativo disponible. La organización por fases encuentra también respaldo empírico, pues el único sistema del corpus que alcanzó producción real no se desplegó de una sola vez: Maestre et al. (2022) documentan una implementación en tres etapas sucesivas. Un único trabajo del corpus se aproxima al mecanismo descrito: Turki et al. (2025) integran un código de respuesta rápida que permite acceder de inmediato al registro correspondiente del diploma en la cadena de bloques, formulación significativa porque el código no conduce al archivo sino al registro, si bien dicho registro reside allí en la cadena y no como etapa institucional previa.

CONCLUSIONES

La revisión de treinta y nueve referencias publicadas entre 2019 y 2026 permite caracterizar el estado de la verificación de certificados académicos mediante cadena de bloques como un campo en expansión antes que en consolidación. La producción se acelera de forma marcada a partir de 2023 y alcanza su

máximo en 2025, pero esa intensificación no se corresponde con un aumento equivalente en los despliegues efectivos: de los veintiocho sistemas documentados, veintiséis no han superado el estadio de prototipo y uno solo cuenta con producción real verificada de manera independiente. Para una institución que evalúe incorporarse a esta línea, el dato pertinente no es el volumen de literatura disponible sino la escasez de experiencias en operación sobre las cuales apoyarse.

El análisis del corpus permite formular una observación sobre el modelo de amenaza que subyace a esta literatura. Los sistemas revisados persiguen, de forma explícita, independizar la verificación de la autoridad central, lo que presupone un emisor cuya palabra no resulta suficiente. La configuración habitual en una institución de educación superior que emite certificados de participación es, sin embargo, la inversa. De este desajuste se sigue que la literatura omita una etapa intermedia, el registro institucional de huellas criptográficas, que carece de sentido bajo el supuesto de un emisor no confiable pero que resuelve el riesgo efectivamente presente en el caso institucional a un costo marginal. Esta constituye la principal aportación conceptual del presente trabajo.

Sobre esa observación se articula el modelo propuesto, organizado en fases que responden a riesgos de naturaleza distinta antes que a consideraciones presupuestarias. Conviene precisar su alcance: el registro institucional no equivale a un sellado de tiempo en sentido técnico ni elimina la necesidad de confiar en la institución emisora, que conserva la capacidad de modificar tanto el documento como su registro. Constituye una garantía sustantiva frente a los riesgos externos, no frente al emisor mismo; son las fases posteriores las que desplazan progresivamente esa dependencia.

Este trabajo se propuso ofrecer al lector institucional un mapa del estado real de la cuestión. El propósito no fue persuadir respecto de su adopción, sino permitir que cada institución determine con prontitud si la línea se ajusta a su propia realidad. Una institución que, tras examinar la evidencia reunida, concluya que el estado de madurez del campo no justifica por el momento una inversión propia, habrá obtenido de esta revisión un resultado tan legítimo como el de aquella que decida lo contrario.

De los resultados se derivan cinco líneas de investigación pendientes. La primera es la validación empírica del modelo mediante el desarrollo de un prototipo de la Fase 1 en el contexto editorial de la Universidad Estatal Amazónica, con medición de su comportamiento en operación real. La segunda es la medición de la dimensión institucional de la adopción, ausente en treinta y siete de los treinta y nueve

trabajos revisados, pese a que las barreras que los propios autores declaran con mayor frecuencia pertenecen al orden institucional antes que al técnico. La tercera es la construcción efectiva de esquemas interinstitucionales, incluida la definición de los criterios de admisión, los mecanismos de gobernanza y el tratamiento de la revocación entre nodos, cuya resolución determina la viabilidad de la Fase 3. La cuarta es el contraste sistemático con la infraestructura de firma electrónica, que permitiría determinar en qué condiciones esta resulta suficiente y a partir de qué umbral se justifica el anclaje distribuido. La quinta es la producción de evidencia en el contexto ecuatoriano, hoy limitada a dos trabajos que no superan el estadio conceptual.

Finalmente, cabe consignar una constatación de orden metodológico surgida durante la propia ejecución del trabajo. La verificación de cada referencia contra su documento original reveló que veintidós de las cuarenta y tres que integraban el corpus en esa etapa contenían algún error de citación, incluidos dos casos en que el identificador digital remitía a un artículo distinto del citado, y uno de esos errores resultó heredado de una fuente del propio corpus. La proporción encontrada sugiere que la verificación directa contra la fuente primaria no constituye una precaución accesoria en una revisión bibliográfica, sino una condición de su validez.

REFERENCIAS BIBLIOGRAFICAS

Aamir, M., Qureshi, R., Khan, F. A., & Huzaifa, M. (2020). Blockchain based academic records verification in smart cities. *Wireless Personal Communications*, 113(3), 1397-1406. https://doi.org/10.1007/s11277-020-07226-0

Abreu, A. W. S., Coutinho, E. F., & Bezerra, C. I. M. (2020). A blockchain-based architecture for query and registration of student degree certificates. En Proceedings of the 14th Brazilian Symposium on Software Components, *Architectures, and Reuse* (pp. 151-160). ACM. https://doi.org/10.1145/3425269.3425285

Awaji, B., Solaiman, E., & Marshall, L. (2020). Blockchain-based trusted achievement record system design. En Proceedings of the 5th International Conference on Information and Education Innovations (pp. 46-51). ACM. https://doi.org/10.1145/3411681.3411689

Berrios Moya, J. A., Ayoade, J., & Uddin, M. A. (2025). A zero-knowledge proof-enabled blockchain-based academic record verification system. Sensors, 25(11), 3450.

https://doi.org/10.3390/s25113450

Caramihai, M., & Severin, I. (2023). A blockchain-based solution for diploma management in universities. *Sustainability*, 15(20), 15169. https://doi.org/10.3390/su152015169

Castro, R. Q., & Au-Yong-Oliveira, M. (2021). Blockchain and higher education diplomas. European Journal of Investigation in Health, *Psychology and Education*, 11(1), 154-167. https://doi.org/10.3390/ejihpe11010013

Cherrafi, A., Elfezazi, S., Chiarini, A., Mokhlis, A., & Benhida, K. (2016). The integration of lean manufacturing, Six Sigma and sustainability: A literature review and future research directions for developing a specific model. *Journal of Cleaner Production*, 139, 828-846. https://doi.org/10.1016/j.jclepro.2016.08.101

Dash, S. P., Jena, A. K., & Murala, D. K. (2025). A Hyperledger-based secure framework for academic certificate authentication using blockchain. *International Journal of Safety and Security Engineering,* 15(6), 1185-1195. https://doi.org/10.18280/ijsse.150610

Dewangan, N. K., Chandrakar, P., Kumari, S., & Rodrigues, J. J. P. C. (2022). Enhanced privacy-preserving in student certificate management in blockchain and interplanetary file system. Multimedia Tools and Applications, 82(8), 12595-12614. https://doi.org/10.1007/s11042-022-13915-8

El-Dorry, A., Reda, M., Abd El Khalek, S., Mohamed, S. E.-D., Mohamed, R., & Nabil, A. (2020). Egyptian universities digital certificate verification model using blockchain. En Proceedings of the 2020 9th International Conference on Software and Information Engineering (pp. 79-83). ACM. https://doi.org/10.1145/3436829.3436864

Evangelista Andrade, A. J., & Amate, F. C. (2025). A decentralized academic certificate issuance system using smart contracts on the Tron network. *International Journal of Computer Science and Information Technology*, 17(6), 53-61. https://doi.org/10.5121/ijcsit.2025.17604

Farabi, A., Khandaker, I., Ahsan, J., Shanto, I. K., Jahan, N., & Khan, M. J. (2025). ShikkhaChain: A blockchain-powered academic credential verification system for Bangladesh [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2508.05334

Fartitchou, M., Lamaakal, I., El Makkaoui, K., El Allali, Z., & Maleh, Y. (2025). BlockMEDC: Blockchain smart contracts system for securing Moroccan higher education digital certificates. IEEE Access, 13, 39152-39175. https://doi.org/10.1109/ACCESS.2025.3546177

Gómez Vieites, Á., Delgado-von-Eitzen, C., & Estévez García, D. (2025). GDPR-compliant academic certification via blockchain: Legal and technical validation of the GAVIN project. Applied Sciences, 15(16), 9191. https://doi.org/10.3390/app15169191

Gresch, J., Bastos Rodrigues, B., Scheid, E. J., Kanhere, S. S., & Stiller, B. (2019). The proposal of a blockchain-based architecture for transparent certificate handling. En Business Information Systems Workshops (Lecture Notes in Business Information Processing, pp. 185-196). Springer. https://doi.org/10.1007/978-3-030-04849-5_16

Guerschberg, L., & Gutiérrez, Y. E. (2025). Blockchain en la educación superior latinoamericana: Estado actual, aplicaciones y desafíos ético-tecnológicos. *Ciencia Latina Revista Científica Multidisciplinar,* 9(5), 15962-15987. https://doi.org/10.37811/cl_rcm.v9i5.20933

Haque, M., Kumar, V. V., Singh, P., Goyal, A. A., Upreti, K., & Verma, A. (2023). A systematic meta-analysis of blockchain technology for educational sector and its advancements towards Education 4.0. *Education and Information Technologies*, 28(10), 13841-13867. https://doi.org/10.1007/s10639-023-11744-2

Hsu, C.-S., Tu, S.-F., & Chiu, P.-C. (2022). Design of an e-diploma system based on consortium blockchain and facial recognition. *Education and Information Technologies*, 27(4), 5495-5519. https://doi.org/10.1007/s10639-021-10840-5

Kamišalić, A., Turkanović, M., Mrdović, S., & Heričko, M. (2019). A preliminary review of blockchain-based solutions in higher education. En Learning Technology for Education Challenges (Communications in Computer and Information Science, pp. 114-124). Springer. https://doi.org/10.1007/978-3-030-20798-4_11

Kumutha, K., & Jayalakshmi, S. (2022). Blockchain technology and academic certificate authenticity: A review. En Expert Clouds and Applications (Lecture Notes in Networks and Systems, pp. 321-334). Springer. https://doi.org/10.1007/978-981-16-2126-0_28

Le, M.-Q., Le, H.-D., Dinh-Duc, A. V., & Tran, T.-T. (2023). IU-TransCert: A blockchain-based system for academic credentials with auditability. En Proceedings of the 12th International Symposium on Information and Communication Technology (pp. 746-753). ACM. https://doi.org/10.1145/3628797.3628822

Maestre, R. J., Bermejo Higuera, J., Gámez Gómez, N., Bermejo Higuera, J.-R., Sicilia Montalvo, J.-A., & Orcos Palma, L. (2022). The application of blockchain algorithms to the management of education certificates. Evolutionary Intelligence, 16(6), 1967-1984. https://doi.org/10.1007/s12065-022-00812-0

Manoj, R., Joshi, S., Dabholkar, U., Panicker, G. P., Kuriakose, K. P., Zaguia, A., & Khan, M. M. (2021). Blockchain ecosystem for credit transfer in education. Mathematical Problems in Engineering, 2021, 8526456. https://doi.org/10.1155/2021/8526456

Molina, F., Betarte, G., & Luna, C. (2020). A blockchain based and GDPR-compliant design of a system for digital education certificates [Preprint]. arXiv. https://arxiv.org/abs/2010.12980

Morales-Morales, M., Rosero-Correa, L., & Morales-Cardoso, S. (2020). Registro de títulos académicos mediante una aplicación basada en Blockchain y Smart Contracts. *Revista Cátedra*, 3(2), 73-98. https://doi.org/10.29166/catedra.v3i2.2200

Nadeem, N., Hayat, M. F., Qureshi, M. A., Majid, M., Nadeem, M., & Janjua, J. (2023). Hybrid blockchain-based academic credential verification system (B-ACVS). Multimedia Tools and Applications, 82(28), 43991-44019. https://doi.org/10.1007/s11042-023-14944-7

Organización de Estados Iberoamericanos. (2026). La tecnología blockchain en Iberoamérica: Del potencial tecnológico a los desafíos de su adopción (Papeles del Observatorio N.º 30). Observatorio Iberoamericano de la Ciencia, la Tecnología y la Sociedad. https://oei.int

Quinde Paucar, J. J., Beltrán Fuentes, F. P., Pico Barrera, F. M., & Benavides Villarreal, D. (2025). Blockchain para la certificación y trazabilidad de competencias en educación superior. Polo del Conocimiento, 10(11). https://doi.org/10.23857/pc.v10i11.10643

Rani, P., Sachan, R. K., & Kukreja, S. (2024). A systematic study on blockchain technology in education: Initiatives, products, applications, benefits, challenges and research direction. Computing, 106(2), 405-447. https://doi.org/10.1007/s00607-023-01228-z

RedCLARA. (2024). Proyecto Diploma: Emisión de certificaciones y diplomas académicos verificados a través de blockchain en América Latina y el Caribe. Cooperación Latino Americana de Redes Avanzadas. https://www.redclara.net

Reis-Marques, C., Figueiredo, R., & de Castro Neto, M. (2021). Applications of blockchain technology to higher education arena: A bibliometric analysis. *European Journal of Investigation in Health, Psychology and Education*, 11(4), 1406-1421. https://doi.org/10.3390/ejihpe11040101

Rustemi, A., Dalipi, F., Atanasovski, V., & Risteski, A. (2023). A systematic literature review on blockchain-based systems for academic certificate verification. IEEE Access, 11, 64679-64696. https://doi.org/10.1109/ACCESS.2023.3289598

Rustemi, A., Dalipi, F., Atanasovski, V., & Risteski, A. (2024). DIAR: A blockchain-based system for generation and verification of academic diplomas. Discover Applied Sciences, 6, 297. https://doi.org/10.1007/s42452-024-05984-1

Said, S. H., Sinde, R., Kosia, E. N. M., & Dida, M. (2025). A comprehensive blockchain-based system for educational qualifications management and verification to counter forgery. IEEE Access. https://doi.org/10.1109/ACCESS.2025.3542545

Sai Ramya, N., Lasya, V., & Michael, A. A. (2026). Blockchain based academic certification verification system. En Proceedings of the International Conference on Intelligent Systems for a Sustainable Future (Atlantis Highlights in Intelligent Systems, pp. 944-955). Atlantis Press. https://doi.org/10.2991/978-94-6239-693-7_91

Tepelidis, A., Mitsopoulou, E. E., Patenidis, A. T., Votis, K., & Tzovaras, D. (2023). A multi-blockchain system for verifiable academic credentials. En Open Science in Engineering (Lecture Notes in Networks and Systems, pp. 917-926). Springer. https://doi.org/10.1007/978-3-031-42467-0_86

Tepelidis, A., Mitsopoulou, E. E., Patenidis, A. T., Livitckaia, K., Votis, K., & Tzovaras, D. (2025). BlockAdemiC: A digital distributed verification system for educational activities in higher education. ACM Distributed Ledger Technologies: Research and Practice, 4(3), 1-19. https://doi.org/10.1145/3703463

Terzi, S., Stamelos, I., Votis, K., & Tsiatsos, T. (2022). A life-long learning education passport powered by blockchain technology and verifiable digital credentials: The BlockAdemiC project. En Software Engineering and Formal Methods. SEFM 2021 Collocated Workshops (Lecture Notes in Computer Science, pp. 249-263). Springer. https://doi.org/10.1007/978-3-031-12429-7_18

Turki, M., Kallel, S., & Jmaiel, M. (2025). EduCheck: Ensuring diploma authenticity using blockchain technology. En Service-Oriented Computing – ICSOC 2024 Workshops (Lecture Notes in Computer Science, pp. 270-274). Springer. https://doi.org/10.1007/978-981-96-7423-7_31

Vidal, F. R., Gouveia, F., & Soares, C. (2020). Blockchain application in higher education diploma management and results analysis. Advances in Science, *Technology and Engineering Systems Journal,* 5(6), 871-882. https://doi.org/10.25046/aj0506104