Investigación

Blockchain para asegurar la integridad y trazabilidad en la cadena de custodia de evidencia digital en informática forense: un estudio de mapeo sistemático

Blockchain for Ensuring Integrity and Traceability in the Chain of Custody of Digital Evidence in Computer Forensics: A Systematic Mapping Study

Pablo A. Vaca
Universidad de Nariño, Colombia
pabloandres@udenar.edu.co
https://orcid.org/0009-0002-2886-9456
Edgar R. Dulce-Villarreal
Universidad Nacional Abierta y a Distancia, Colombia
edgar.dulce@unad.edu.co
https://orcid.org/0000-0003-1995-6718

Recepción: 29 Marzo 2024
Aprobación: 15 Julio 2024
Publicación: 01 Agosto 2024

Acceso abierto diamante

Abstract

The incorporation of blockchain as a strategy to improve information security in various sectors of society has been identified as a potential solution to reduce the risks associated with data processing on the Internet. Ensuring chain of custody in forensic investigations is essential to preserve the record and provenance of digital evidence. However, the lack of research on the development and implementation of solutions that integrate blockchain for chain of custody hinders its application and adoption. Therefore, this research aimed to classify the characteristics of blockchain that allow to guarantee the integrity and traceability of digital evidence in the chain of custody process, through a literature review based on a Systematic Mapping Study. The study described the concepts and current status of the blockchain in relation to chain of custody. The findings revealed various frameworks, proofs of concept, prototypes, and protocols that proposed blockchain applications in the recording, exchange, and traceability of digital evidence in different contexts and the benefits, limitations, and challenges associated with their implementation. As a final conclusion, it highlights the close relationship between integrity and traceability as fundamental properties for the construction of blockchain applications and provides a solid foundation of information that can serve as a reference for future research.

Keywords: Blockchain, chain of custody, digital evidence, digital forensics, data integrity.

Resumen

La incorporación de blockchain como estrategia para mejorar la seguridad de la información en diversos sectores de la sociedad se ha identificado como una potencial solución para reducir los riesgos asociados con el tratamiento de datos en Internet. Garantizar la cadena de custodia en investigaciones forenses es esencial para preservar el registro y procedencia de la evidencia digital. No obstante,

Notas de autor
pabloandres@udenar.edu.co

la falta de investigación en el desarrollo e implementación de soluciones que integren blockchain para la cadena de custodia dificulta su aplicación y adopción. Por ello, esta investigación tuvo como objetivo clasificar las características de blockchain que permiten garantizar la integridad y trazabilidad de la evidencia digital en el proceso de cadena de custodia, mediante una revisión de literatura basada en un Estudio de Mapeo Sistemático. El estudio describió los conceptos y estado actual de blockchain en relación con la cadena de custodia. Los hallazgos revelaron diversos marcos, pruebas de concepto, prototipos y protocolos que propusieron aplicaciones de blockchain en el registro, intercambio y trazabilidad de evidencia digital en diferentes contextos, así como los beneficios, limitaciones y desafíos asociados con su implementación. Como conclusión final, se destaca la estrecha relación entre integridad y trazabilidad como propiedades fundamentales para la construcción de aplicaciones blockchain, además de proporcionar una base sólida de información que pueda servir de referencia para futuras investigaciones.

Palabras clave: Blockchain, cadena de custodia, evidencia digital, informática forense, integridad de los datos.

Highlights

Blockchain es una tecnología disruptiva que puede garantizar la integridad y trazabilidad en la cadena de custodia en evidencia digital.
Las plataformas de blockchain Hyperledger y Ethereum se clasifican como las más adecuadas para el desarrollo de aplicaciones descentralizadas.
Los estudios demuestran que en la implementación de aplicaciones blockchain para la cadena de custodia se debe cumplir las características de privacidad, autorización e inmutabilidad.
Los desafíos y limitaciones más abordados en los estudios son el cumplimiento normativo, investigaciones transfronterizas, la seguridad, el almacenamiento y la preservación de datos.

Highlights

Blockchain is a disruptive technology that can ensure integrity and traceability in the chain of custody of digital evidence.
Hyperledger and Ethereum blockchain platforms are classified as the most suitable for the development of decentralized applications.
Studies show that the implementation of blockchain applications for chain of custody must meet the characteristics of privacy, authorization, and immutability.
The challenges and limitations most addressed in studies are regulatory compliance, cross-border investigations, security, data storage, and preservation.

1. INTRODUCCIÓN

La transformación del mundo en la actualidad está siendo impulsada por la adopción de tecnologías emergentes como el Internet de las cosas, la inteligencia artificial, la realidad virtual, la hiperconectividad y blockchain (BC) [1]. Este avance se ve complementado por el rápido crecimiento de la información digital [2], resultado del uso extendido de dispositivos inteligentes en diversos sectores de la sociedad, como la asistencia sanitaria, el comercio electrónico, y la agricultura [3]. Esto conlleva un aumento progresivo de los delitos informáticos, que a su vez implica la necesidad de sistemas forenses innovadores capaces de manejar nuevos tipos de datos electrónicos, los cuales se convierten en los materiales más importantes en una investigación forense [4]. La evidencia digital ha planteado desafíos para los métodos y técnicas forenses tradicionales, reduciendo su efectividad y dificultando la credibilidad y fiabilidad de dicha evidencia en procesos legales [5]. Según [6], la ciencia forense digital necesita desarrollar nuevos enfoques que faciliten la identificación, procesamiento y validación de la evidencia, la cual se origina a partir de diversas fuentes digitales que son aprovechadas por los delincuentes para cometer delitos informáticos [7]. De acuerdo con [8], la falta de claridad en las regulaciones de ciberseguridad y la aplicación de procesos adecuados en las investigaciones, particularmente en el estricto cumplimiento de la cadena de custodia (CoC, por sus siglas en inglés), pueden invalidar las pruebas digitales debido a la falta de conformidad con los sistemas de gobernanza en el ciberespacio.

La CoC se describe como el conjunto detallado de procedimientos establecidos con el propósito primordial de asegurar y garantizar la correcta manipulación de pruebas digitales desde su obtención inicial hasta su entrega ante la autoridad judicial, con el fin de preservar su integridad y valor probatorio [9]. Este conjunto de medidas se implementa para evitar cualquier manejo inadecuado en la recolección, registro, almacenamiento, análisis y documentación detallada de cada paso realizado, donde se puede comprometer la validez de la evidencia durante la investigación forense [10], [11]. Según la ISO 27037 [12], el proceso de CoC define 5

etapas: Identificación, Adquisición, Preservación, Análisis y Presentación, las cuales proporcionan la trazabilidad completa y transparente de todo el proceso investigativo. La norma recomienda directrices para asegurar que los investigadores forenses digitales preserven la integridad de las pruebas digitales durante las etapas de recolección de datos, por medio de metodologías de análisis diseñadas para favorecer la admisibilidad de las pruebas durante los procesos judiciales, en conformidad con sus principios fundamentales [13], [14]. En la primera etapa se identifican y registran todas las pruebas y evidencias digitales relacionadas con la investigación. Durante la etapa de Adquisición, se recopilan y obtienen las pruebas digitales asegurando que se mantenga la integridad de los datos. En la fase de Preservación, se almacenan y conservan las pruebas digitales de forma segura para evitar cualquier alteración, destrucción o pérdida. Para la etapa de Análisis, se examinan y se analizan las pruebas digitales con el objetivo de extraer información relevante para la investigación. Por último, en la etapa de Presentación, se documenta y se presenta la evidencia digital de manera que sea admisible en un tribunal o ante las autoridades pertinentes. Estas etapas definen un proceso completo, el cual garantiza la integridad, la trazabilidad y la confiabilidad de la evidencia digital en el contexto de investigaciones forenses [15]. Sin embargo, este proceso evidencia problemas asociados con los avances tecnológicos y el alcance de las pruebas digitales [10], [15]. Por sus características, las evidencias pueden ser fácilmente copiadas, modificadas, borradas, transferidas e incluso contaminadas con otros datos [16].

Según [17], los desafíos de las pruebas digitales se enmarcan en aspectos relacionados con en el almacenamiento en la nube [18], la multitenencia [19], la geolocalización [19] y la falta de normatividad legal [16] para el tratamiento de información digital. Por otra parte, [20] afirma que la introducción de nuevas tecnologías como la computación en la nube y el Internet de las cosas están impulsando una revolución digital que, a su vez, ha dado lugar a nuevas vulnerabilidades que comprometen la seguridad de los datos, aumentando así el riesgo de múltiples ataques cibernéticos.

En el estudio llevado a cabo en [21], se presenta un modelo genérico para el proceso de análisis de la ciberdelincuencia en el Internet de las cosas. Esta propuesta se centra en clasificar las pruebas de manera anticipada según su relevancia y su relación con delitos anteriores, así como en la gravedad de las pruebas en términos de la probabilidad de ocurrencia de un ciberdelito. El enfoque destaca la importancia de modelos que contribuyan a ahorrar tiempo y esfuerzo en el proceso de automatización en investigación forense.

En la revisión de la literatura sobre la CoC en el ámbito de la medicina forense realizada por [22], se hace énfasis en su establecimiento y mantenimiento. El trabajo resalta la importancia de proteger la integridad y la validez de las pruebas, especialmente ante la carencia actual de prácticas sólidas que sean aplicables tanto a pruebas físicas como a pruebas digitales. La definición de modelos es fundamental para garantizar la integridad y trazabilidad de las pruebas a lo largo de su ciclo de vida en la investigación, como describen en la metodología propuesta en [23] para preservar y evaluar la integridad de una prueba digital dentro de la CoC mediante un sistema de localización.

Aunque hay varios estudios que proporcionan distintos enfoques para abordar los desafíos de la CoC digital en los procesos forenses modernos [24]-[26], continúan existiendo dificultades y limitaciones. Por consiguiente, se requiere llevar a cabo nuevas investigaciones centradas en implementaciones prácticas que puedan adaptarse a estos desafíos.

La tecnología BC surge como una solución de registro descentralizado y persistente, que permite la creación y mantenimiento de un registro seguro y transparente de transacciones o datos, distribuido en múltiples nodos de una red [27]. Está tecnología tiene el potencial para transformar el panorama de las investigaciones forenses. Al aprovechar sus características, es posible desarrollar sistemas y mecanismos capaces de verificar la validez y autenticidad de los procesos utilizados en la CoC para registrar, almacenar, preservar y transmitir pruebas digitales garantizando la inmutabilidad, integridad y trazabilidad de las evidencias durante todo el proceso forense.

La literatura presenta un avance significativo y hay un interés creciente en explorar la aplicación de esta tecnología en el ámbito forense. En el estudio [28], se analiza la relación entre la tecnología BC y la

investigación forense de dispositivos móviles, resaltando tanto los retos como los beneficios asociados. Además, propone un marco forense basado en BC para registrar de forma confiable los hallazgos forenses, con el objetivo de resolver los problemas relacionados con la privacidad, la seguridad y la colaboración entre los equipos forenses. De igual forma, en [29] se enfocan en asegurar la inmutabilidad de las pruebas, y así validar que esta tecnología se convierte en una de las opciones principales para mantener y rastrear la CoC forense. Su propuesta propone un sistema basado en BC que permita gestionar la evidencia digital desde el momento que se recogen hasta su presentación como prueba ante el tribunal.

Aunque existe un incremento en investigaciones que consideran la tecnología BC como una solución prometedora para la CoC en evidencia digital, estás aún se encuentran en etapas tempranas de desarrollo, motivo por el cual existen ciertos vacíos y desafíos por abordar. En consecuencia, este artículo se centra en revisar y analizar la relevancia de la tecnología BC para garantizar la integridad y trazabilidad de la evidencia digital en el proceso de CoC a través de un Estudio de Mapeo Sistemático (SMS, por sus siglas en inglés), el cual es una versión extendida del trabajo presentado originalmente como ponencia en [30]. El propósito es clasificar las características de BC como mecanismo para implementar BC en el dominio de la CoC para futuros trabajos y aplicaciones que permitan aprovechar su potencial, así como conocer sus limitaciones y desafíos. El artículo está organizado de la siguiente manera: La Sección 2 describe el diseño metodológico utilizado en esta investigación. La Sección 3 muestra los resultados y la discusión. Las conclusiones se detallan en la Sección 4.

2. METODOLOGÍA

En este estudio se aborda la metodología de [31] y las pautas descritas en [32] para realizar el SMS. El cual se centra en explorar el estado actual de BC en el dominio de la CoC como mecanismo para garantizar la integridad y trazabilidad en evidencia digital. El SMS permitió recopilar y clasificar las características utilizadas en el diseño y construcción de BC específicas para el dominio de la CoC en evidencia digital. También se identificó los beneficios, limitaciones y desafíos presentados por los autores, que permitirán aclarar el panorama actual de BC con relación a la CoC, además de apoyar futuros trabajos en este ámbito. El SMS se divide en diferentes pasos secuenciales, aplicación de criterios y filtros como se muestra en la Figura 1.

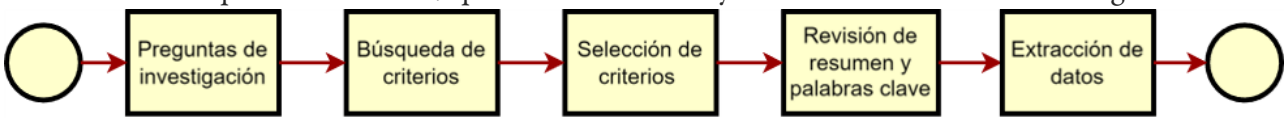

Figura 1.
Proceso de mapeo sistemático basado en [31].
Fuente: elaboración propia.

2.1 Definición de las preguntas de investigación

El primer paso de este SMS es definir las preguntas de investigación (RQ, por sus siglas en inglés) que pretenden proporcionar respuestas sobre la tecnología BC en el dominio de la CoC como mecanismo para garantizar la integridad y trazabilidad en evidencia digital. Para la búsqueda de estudios primarios relacionados, se definieron las siguientes RQ, como se observa en la Tabla 1.

Tabla 1.
Preguntas de investigación para mapeo sistemático.

Id.	Pregunta
RQ1	¿Qué tipo de BC (privada, pública, otras) y qué mecanismos de consenso se utilizan para el diseño y construcción de aplicaciones enfocadas en el proceso de CoC en evidencia digital?
RQ2	¿Qué beneficios ofrece BC para la CoC en evidencia digital en términos de integridad y trazabilidad?
RQ3	¿Cuáles son los desafíos y limitaciones existentes en la implementación de BC para la CoC en evidencia digital?
RQ4	¿Cuáles son las perspectivas futuras y tendencias emergentes en la aplicación de BC para el proceso de CoC en evidencia digital?

Fuente: elaboración propia.

2.2 Definición de la cadena de búsqueda

Los estudios primarios se identificaron mediante la búsqueda y recopilación de todos los trabajos de investigación relacionados con BC en relación con la CoC como mecanismo para garantizar la integridad y trazabilidad en evidencia digital, en función de los términos de búsqueda específicos. Para ello, se usó la metodología PICOC [33], para combinar los elementos esenciales para estructurar y representar los términos: población, intervención, comparación, resultados y contexto del objeto de estudio, que relacionados permitan definir las RQ y la cadena de búsqueda [34] de forma correcta. Las palabras claves identificadas mediante la estrategia PICOC se pueden ver en la Tabla 2.

Tabla 2
Identificación de palabras clave utilizando la estrategia PICOC

Término	Palabras clave
Población	Blockchain
Intervención	Chain of custody, CoC
Comparación y resultado	Integrity, Traceability
Contexto	Digital evidence

Fuente: elaboración propia.

Siguiendo estas directrices, se elaboró la siguiente cadena de búsqueda de palabras clave definidas, la cual relaciona la tecnología BC con la CoC en evidencia digital, enfocada en la integridad y trazabilidad, como se detalla en la Tabla 3. Estos términos abarcan todo el contexto que se quiere revisar en esta investigación.

Tabla 3
Cadena de búsqueda Fuente elaboración propia

Cadena de búsqueda
(blockchain) AND ("chain of custody" OR coc)AND(integrity OR traceability) AND ("digital evidence")

Fuente: elaboración propia.

Una vez identificadas las palabras clave para la tarea de búsqueda, se procedió a la selección de las bases de datos bibliográficas, basados en [35], que señala las más relevantes y con mayor cantidad de fuentes de citas en el ámbito de la informática y la ingeniería. En este sentido, se escogió las siguientes bases datos para esta revisión: ACM Digital Library, IEEEXplore y Scopus.

2.3 Definición de criterios de selección: Inclusión y Exclusión

En la Tabla 4 se definen los criterios de inclusión (I) y exclusión (E) para determinar que trabajos son relevantes o no para este estudio [36].

Tabla 4
Criterios de inclusión y exclusión

Id.	Inclusión	Id.	Exclusión
I1	Artículos publicados en los últimos cinco años (2019 - 2023).	E1	Informes técnicos, resúmenes, encuestas (literatura gris) y estudios secundarios (SMS).
I2	Si hay varios artículos relacionados con el mismo estudio, sólo se seleccionará el más reciente.	E2	Artículos escritos en idiomas distintos del inglés.
I3	Si un artículo describe más de un estudio, cada estudio se evalúa individualmente.	E3	Artículos que no presenten estudios relacionados con la BC, CoC, integridad, trazabilidad, evidencia digital, mecanismo de consenso o sinónimos.
I4	Si existen versiones abreviadas y completas del mismo estudio, se selecciona la versión completa.	E4	Sólo artículos de revistas, conferencias y Early Access.

Fuente: elaboración propia.

2.4 Búsqueda y extracción de datos de documentos relevantes

Una vez definidos los criterios de inclusión y exclusión, el siguiente paso es la búsqueda de documentos en las bases de datos bibliográficas mediante la cadena de búsqueda detallada en la Tabla 3, y posteriormente realizar la revisión del título, resumen y palabras clave de cada uno de los estudios seleccionados para identificar artículos que puedan ser de interés y descartar aquellos que no cumplan con los criterios de inclusión y exclusión [31] definidos en la Tabla 4. En el diagrama de burbujas que se muestra en la Figura 2, se reporta el número de artículos por cada una de las bases de datos consultadas.

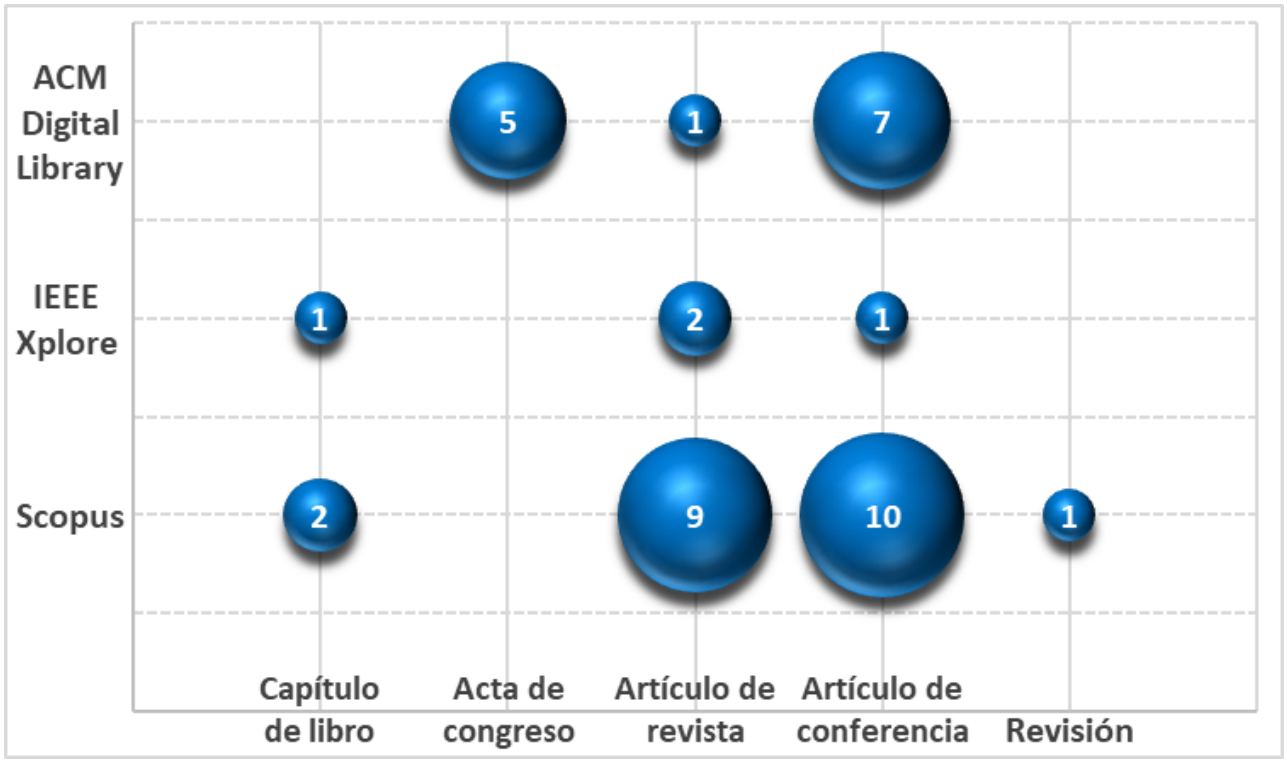

Figura 2.
Número de trabajos por tipo obtenidos en las bases de datos.
Fuente: elaboración propia.

Realizado el paso anterior, se procede a leer la introducción, resultados y conclusiones de los artículos seleccionados considerando los criterios de inclusión y exclusión. Después de aplicar los filtros, con el conjunto final de trabajos relevantes para este estudio, se procede a su lectura completa y análisis que se presenta en la Sección 3. Resultados y discusión, teniendo en cuenta su diseño metodológico, aplicación práctica y resultados presentados. Realizado el proceso de selección, se lleva a cabo una tarea adicional que implica la evaluación de la calidad en los artículos relacionados, basado en [37], [38], ver Tabla 5.

Tabla 5
Criterios de evaluación de la calidad

Id.	Categoría	Criterio de calidad	Escala de ponderación
C1	Calidad del informe	Los objetivos y las RQ se describen de forma explícita, clara y pertinente.	Si cumple (2 puntos). Si cumple parcialmente, (1 punto). Si no cumple (0 puntos).
C2	Rigor	La investigación presenta un diseño metodológico que permite alcanzar los objetivos.	Si cumple (2 puntos). Si cumple parcialmente, (1 punto). Si no cumple (0 puntos).
C3	Rigor	El trabajo define la plataforma BC y mecanismo de consenso que utilizó.	Si cumple (2 puntos). Si cumple parcialmente, (1 punto). Si no cumple (0 puntos).
C4	Rigor	El trabajo propone una solución aplicada basada en BC.	Para estudios con aplicación (1 punto). Para estudios teóricos (0 puntos).
C5	Credibilidad	Los resultados presentados son claros y coherentes con el diseño metodológico.	Si cumple (2 puntos). Si cumple parcialmente, (1 punto). Si no cumple (0 puntos).
C6	Relevancia	El estudio es valorado por otros investigadores (Número de citas artículo).	Mayor o igual a 6 citas (Alta, 2 puntos). Entre 1 y 5 citas (Media, 1 punto). Sin citas (Baja, 0 puntos).

Fuente: elaboración propia.

Estos criterios se consideraron relevantes para el análisis del estudio y las RQ que guían esta investigación, porque apoyaron el cumplimiento, la calidad de los recursos y condujeron a las respuestas de las RQ definidas. Al final del proceso de evaluación de la calidad, se mantuvieron los 18 artículos seleccionados durante la fase de extracción de datos, indicando que el 100 % de las referencias aportan de manera significa en la investigación.

Durante el proceso de extracción de información, se realizó un análisis cualitativo y cuantitativo con los datos obtenidos en los estudios [39], con el propósito de clasificar las contribuciones de cada artículo que permitieron dar respuesta a las preguntas de investigación (RQ) planteadas en el mapeo sistemático (Sección 3. Resultados y discusión). Entre los resultados se incluye el número de publicaciones por año, tipos de blockchain, entornos de implementación, entre otros análisis procesados mediante una hoja de cálculo.

3. RESULTADOS Y DISCUSIÓN

El objetivo de este trabajo es explorar las características utilizadas en el diseño y construcción de BC en el dominio de la CoC en evidencia digital, como mecanismo para garantizar integridad y trazabilidad, así como describir sus beneficios y limitaciones, y discutir sobre desafíos, perspectivas futuras y tendencias emergentes. La Figura 3 muestra el proceso de refinamiento, el cual se describe a continuación: Inicialmente, al buscar en las bases de datos seleccionadas, se obtuvieron 39 artículos. De los cuales, se identificó que 6 de ellos se encuentran almacenados en más de una base de datos, que conllevó a eliminar los duplicados, quedando solo una copia de cada trabajo en los registros. Así, para el siguiente paso, quedaron 33 artículos por analizar. A continuación, se aplican los criterios de inclusión y exclusión (I1 + E1 + E2) en los 33 trabajos, incluyendo los publicados en los últimos cinco (5) años y, excluyendo los registros que no corresponden a artículos publicados en revistas, congresos o capítulos de libros, además de los escritos en idiomas distintos al inglés, quedando 21 artículos. Se aplican los criterios de inclusión y exclusión (I2 + I3 + I4 + E3 + E4) en los 21 artículos, leyendo su introducción, resultados y conclusiones. Donde se identificó 1 artículo que hacía referencia a un mismo

trabajo. Además, se descartaron 2 documentos que no eran accesibles a su versión completa, obteniendo como resultado 18 artículos relevantes con el tema de investigación. Estos 18 artículos se utilizaron como evidencia para responder las RQ. La lista de artículos finales se encuentra en la Sección 6, Referencias. Para la revisión y análisis de los documentos completos, y evitar sesgos por parte del investigador, se contó con el apoyo de un experto externo a la investigación. En la Figura 3, se resume todo el proceso de clasificación de los 18 trabajos finales.

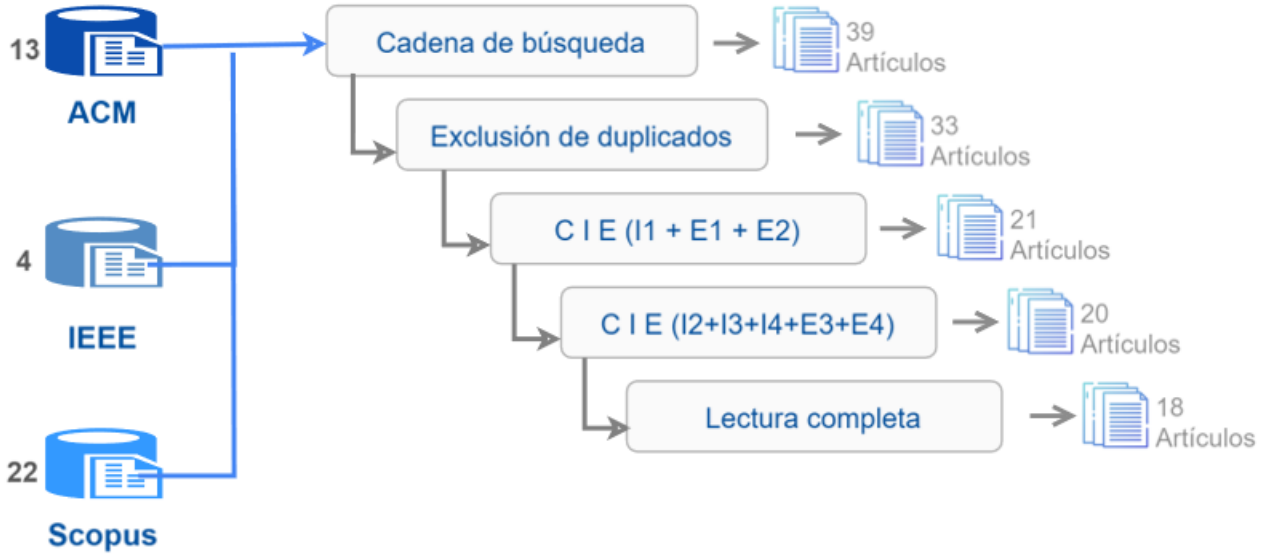

Figura 3.
Proceso de filtrado de artículos, basado en [40].
Fuente: elaboración propia.

3.1 Aspectos generales

Con la información extraída de los 18 artículos seleccionados, se evidencia una escasez de estudios en la literatura existente respecto a la implementación de la tecnología BC en el dominio de la CoC como mecanismo para garantizar la integridad y trazabilidad en la evidencia digital. Esta ausencia de investigación convierte este tema en un reto y una oportunidad para profundizar en este campo poco explorado [38], permitiendo generar nuevo conocimiento que contribuya a su avance y desarrollo.

De acuerdo con la Figura 4, el primer aspecto identificado fue la clasificación del tipo de publicación (capítulo de libro, artículo de revista y artículo de conferencia) de los artículos seleccionados, teniendo en cuenta la base de datos de donde se obtuvieron. Se constata que el número de artículos de conferencias (11 artículos) es el más frecuente. Este resultado destaca la importancia de los eventos científicos y académicos para la difusión de investigaciones sobre la tecnología BC en relación con la CoC en evidencia digital, así como para dar a conocer los últimos avances en investigación aplicados sobre este tema en distintas áreas del conocimiento. Seguidos se encuentran los artículos de revistas (6 artículos), lo cual es positivo considerando la baja productividad. Además, este tipo de documentos son los más rigurosos en cuanto a revisión por pares y editores. Así, estás dos primeras clasificaciones de estudios representa el 94,4 % de los documentos. Por último, se identificó un capítulo de libro.

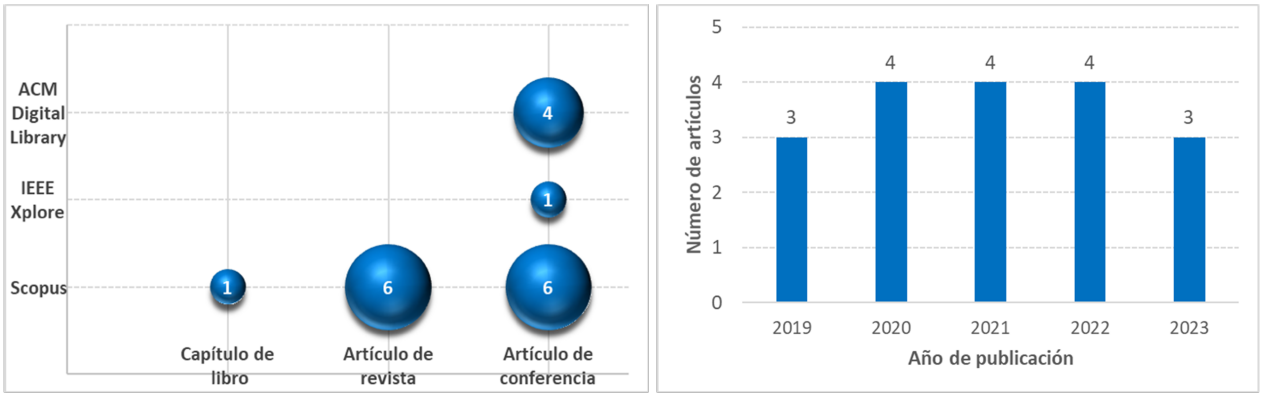

Figura 4.

Aspectos generales.

a. Número de artículos por tipo. b. Estudios finales por año.

Fuente: elaboración propia.

El segundo aspecto general identificado hace referencia a la frecuencia de publicación de los artículos. Se encontró que, a partir del año 2019, existe una tendencia gradualmente creciente, lo cual indica un interés e importancia continua en explorar el tema de investigación en los últimos 5 años por parte de la comunidad académica. Como se puede apreciar en la Figura 4, esta tendencia al alza se observa claramente, teniendo en cuenta que la revisión se realizó a mediados del año 2023.

Como se presenta en la Figura 5 y la Tabla 6, otro aspecto importante es la procedencia de los artículos, identificada mediante la ubicación geográfica de cada autor de los documentos revisados. En la Figura 5, se destaca la presencia de autores tanto de Europa como Asia, cada continente con una contribución del 40 % en los artículos. Entre los países con mayor incidencia en la publicación de estudios se encuentran el Reino Unido (4 artículos), India (4 artículos) y España (2 artículos), lo cual evidencia el liderazgo y la tendencia en la investigación de este tema por parte de la comunidad académica y científica internacional, ver Tabla 6. Además, se resalta la contribución y participación de autores de diferentes países relacionados en los estudios enfocados en BC como mecanismo para garantizar CoC en evidencia digital. Este hecho refleja los esfuerzos tanto académicos como gubernamentales dedicados a este tipo de investigación.

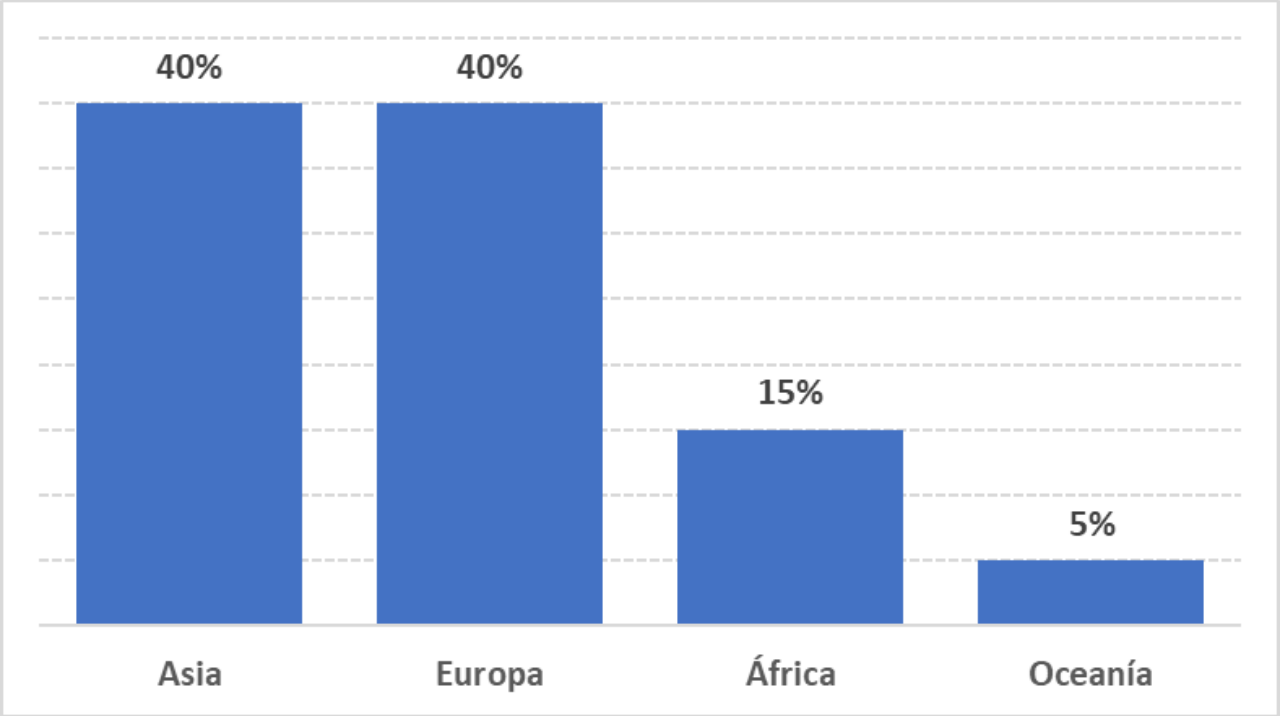

Figura 5.
Publicación de artículos por continente.
Fuente: elaboración propia.

Tabla 6
País de adscripción de los autores por artículo

Ref.	País	Número de autores	Continente
[41]	China	4	Asia
[42]	Egipto	5	África
[43]	Emiratos Árabes, Túnez	3, 1	Asia, África
[44], [45]	España	6	Europa
[46]-[49]	India	11	Asia
[50]	Indonesia	2	Asia
[51]	Italia	3	Europa
[52]	Nigeria	4	África
[53]-[55]	Reino Unido	8	Europa
[17]	Reino Unido, Noruega, Australia	2, 1, 1	Europa, Oceanía
[56]	Suiza	4	Europa
[57]	Taiwán	1	Asia

Fuente: elaboración propia.

Por el contrario, es relevante destacar la falta de participación de autores procedentes de América del Sur. Esto indica que el tema de investigación se está extendiendo en países desarrollados como Reino Unido y España, lo cual demuestra un creciente interés y compromiso por la adopción de tecnologías emergentes. Mientras que, en otros países en vías de desarrollo como Colombia, se observa una menor integración y

generación de conocimiento en estas tecnologías, que evidencia la necesidad de empezar investigaciones en esta área para fortalecer el desarrollo científico y tecnológico en estos países.

Para esquematizar de forma global los resultados, se presenta en la Tabla 7 una clasificación de los principales resultados encontrados. En ella se observan los 18 documentos junto con el diseño metodológico, las fases de análisis forense involucradas, el entorno de implementación, el estado de avance del estudio y los parámetros de evaluación de cada trabajo.

Centrándose en la primera columna, se evidencia que no existe un factor común al momento de elegir el diseño metodológico de cada estudio. La elección del diseño depende varios factores, entre ellos si el enfoque del trabajo se centra en la aplicación o la implementación de un mecanismo arquitectónico basado en BC. Se destacan los marcos de trabajo como los más recurrentes (6/18 artículos) entre los estudios revisados. Estos marcos proporcionan una mejor estructura y guía para la investigación [17], [47], aportando una mayor coherencia y consistencia en la metodología utilizada, además de facilitar la comparación de resultados con otros estudios. En este sentido, los investigadores pueden optar por diferentes metodologías según las características de su investigación, como el contexto, los objetivos y las limitaciones del estudio.

La segunda columna se refiere a las etapas de análisis forense en las que se enfoca cada estudio, siguiendo los principios establecidos por la normativa ISO/IEC 27037 [12], [46], con el propósito de garantizar la integridad, confidencialidad, disponibilidad y trazabilidad de la evidencia digital en el proceso de la CoC. Lo anterior revela que las fases iniciales (identificación, adquisición y preservación) son frecuentes en los trabajos abordados por los autores, mientras que las etapas de análisis y presentación están relacionadas en estudios que presentan experimentación (10/18 artículos). Lo cual, muestra el interés por investigar en BC como estrategia para asegurar la integridad e inmutabilidad de la evidencia digital desde el inicio del proceso de investigación forense, con el fin de garantizar la CoC y cumplir con los estándares necesarios para su validez.

En cuanto a los entornos de implementación, se observa una limitada descripción de plataformas utilizadas en los trabajos. Un total de ocho estudios emplearon plataformas de BC privadas para el desarrollo de sus propuestas. La elección de estas plataformas está relacionada con las características que ofrecen para operar en entornos controlados [50], [51], lo cual garantizan la seguridad y confidencialidad de los datos. Por otro lado, siete artículos no proporcionan información suficiente para su clasificación [46], [53]. Estos trabajos se encuentran directamente relacionados con estudios teóricos, enfocados en realizar una exploración conceptual en el diseño de arquitecturas basadas en BC. Por último, los trabajos restantes presentan otros entornos de implementación [43], [50].

Para el estado de investigación, se identifica que la mayoría de los trabajos se encuentran en etapa de desarrollo, destacando que el 72,2 % (13/18 artículos) hacen referencia a prototipos, experimentos, pruebas de concepto, simulaciones o proyectos finalizados. Esto resalta la importancia que está tomando la adopción de BC como una herramienta fundamental para garantizar la CoC en evidencia digital [56]. Por otra parte, los trabajos restantes (5/18 artículos) presentan estudios aún en fase de propuesta, lo cual indica la necesidad de realizar estudios aplicados para la CoC que permitan consolidar los avances teóricos. La última columna presenta las características utilizadas para evaluar los trabajos empíricos. Se destaca el parámetro de rendimiento como el más abordado (7/18 artículos), lo cual refleja la importancia de evaluar la eficacia de las aplicaciones para procesar transacciones de manera óptima [17], [51]. También, se abordan la eficiencia y la latencia con tres reportes cada una, y por último se encuentra el costo con dos ocurrencias. Este análisis muestra la importancia de validar los resultados de los estudios en su fase de funcionamiento y contrastar el grado de desempeño de las plataformas BC utilizadas como mecanismo para asegurar el proceso CoC en la evidencia digital.

Tabla 7
Principales aspectos encontrados en los trabajos finales

	Diseño metodológico					Análisis forense ISO/IEC 27037					Entorno de implementación				Estado investigación					Parámetros de evaluación				
Ref.	Arquitectura	Marco de trabajo	Enfoque metodológico	Modelo propuesto	Protocolo	Identificación	Adquisición	Preservación	Análisis	Presentación	Plataforma privada	Laboratorio	Caso hipotético	Estudio de caso	Propuesta	Prototipo	Experimento	Simulación	Prueba de concepto	Finalizado	Rendimiento	Latencia	Eficiencia	Costo
[46]	√					√	√	√	√	√					√									
[42]		√				√	√	√	√	√	√					√					√	√		
[44]			√			√	√	√	√	√	√													
[17]		√				√	√	√				√					√				√	√		
[51]	√					√	√	√	√	√	√					√					√	√		
[41]					√	√	√	√								√					√			
[47]		√				√	√	√	√	√	√				√									
[53]						√	√	√							√									
[43]		√				√	√	√					√					√			√		√	
[56]						√	√	√	√	√									√					
[52]		√					√	√							√									

[54]					√	√	√			√					√			√	√
[50]			√		√	√	√				√		√				√	√	√
[48]	√				√	√	√	√	√							√			
[49]				√	√	√	√	√	√	√			√				√		
[55]				√	√	√	√					√							
[45]				√	√	√	√	√	√	√			√						
[57]		√			√	√	√	√	√	√				√					

Fuente: elaboración propia.

La marca de verificación (√) denota la existencia de esta característica dentro del artículo.

3.2 Tipos de BC y mecanismos de consenso (RQ1)

De acuerdo al contexto en el que se abordan los artículos, para dar respuesta a la RQ1, se realizó un esquema de clasificación que agrupa 4 aspectos sobre los cuales es posible relacionar características que ayudan a clasificar los tipos de BC [58], como se puede observar en la Figura 6. Entre los 18 artículos revisados, una mayoría significativa (13/18 artículos) presentan aplicaciones de BC como apoyo al proceso de CoC y al registro de pruebas forenses. Estas aplicaciones abarcan desde prototipos hasta implementaciones prácticas en diversos contextos [41], [49]. De igual forma, se encuentran cinco estudios teóricos que proporcionan fundamentos conceptuales para explorar posibles aplicaciones de la tecnología BC en el ámbito de la CoC. Este análisis refleja que, a pesar de la baja productividad en la construcción de soluciones basadas en BC para asegurar las pruebas digitales en el proceso de la CoC, existe un creciente interés por parte de la comunidad en investigar y desarrollar soluciones centradas en BC para garantizar la integridad, autenticidad y trazabilidad de los datos en la CoC [38]. En cuanto a la categoría tipo de BC, se destacan las BC autorizadas como las de mayor aplicación, con un total de cinco ocurrencias [17], [41], [49], [50], [52], seguidas de las BC privadas, privadas con autorización y públicas [42], [43], [54], todas ellas con cuatro registros cada una. También, se identifica un estudio que define una BC personalizada [46].

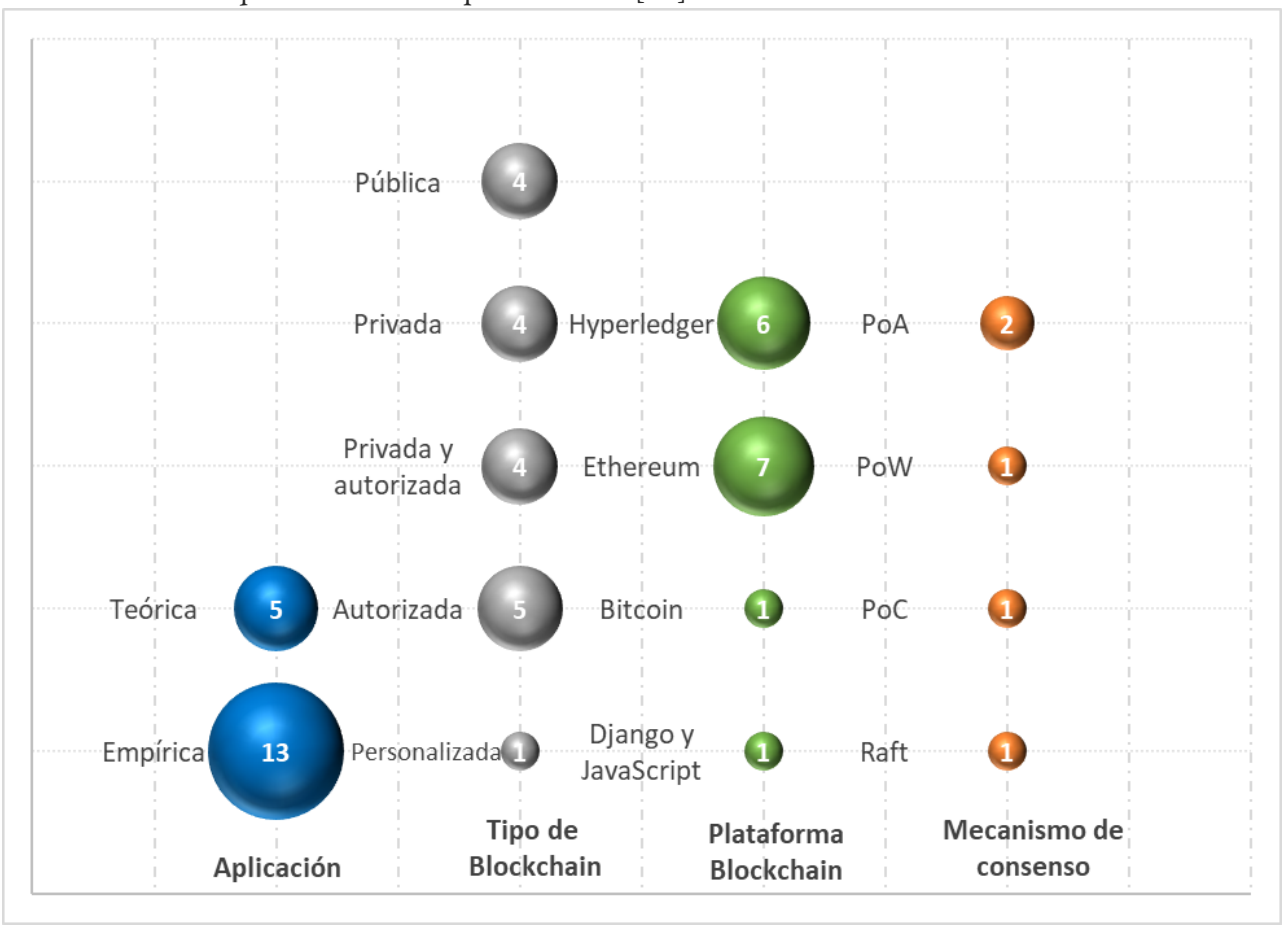

Figura 6.
Clasificación de características de BC.
Fuente: elaboración propia.

Esto permite afirmar que su uso está condicionado por el contexto y el tipo de información que se administre, como lo mencionan algunos autores en sus estudios. Además, se evidencia un alto grado de preferencia por implementaciones que incluyan el factor de autorización, un componente esencial para asegurar la integridad, fiabilidad, trazabilidad y confianza de las pruebas digitales a lo largo del proceso de CoC hasta su presentación en las instancias judiciales, facilitando la detección de cualquier manipulación o acceso no autorizado.

Por otra parte, se observa que Ethereum es la plataforma más destacada, con siete registros, seguida del marco de trabajo Hyperledger con seis registros. Esto refleja el avance y madurez de estas plataformas BC y su capacidad para adaptarse a diferentes entornos de seguridad, incluyendo el campo de la CoC en pruebas digitales [59], [60]. Asimismo, estas plataformas ofrecen funcionalidades de contratos inteligentes, mecanismos de consenso y escalabilidad. Además, proporcionan una variedad de aplicaciones para entornos privados y son compatibles con capas de control de acceso y autenticación, requisitos necesarios en sistemas encargados de garantizar el proceso CoC. Con respecto a los mecanismos de consenso, aunque son pocos los autores que abordan de forma explícita el mecanismo utilizado en sus estudios evidencian que se encuentran estrechamente vinculados con el contexto de aplicación y el tipo de BC utilizado. Entre las opciones descritas se incluyen la prueba de autoridad (PoA, por sus siglas en inglés) [42], [51], la prueba de trabajo (PoW, por sus siglas en inglés) [56], la prueba de capacidad (PoC, por sus siglas en inglés) [49] y el algoritmo Raft [43], que por su naturaleza tienen la capacidad de resistir ataques y contribuir a fortalecer la seguridad de la CoC y preservar la inmutabilidad de los datos.

El análisis de las categorías descritas resalta la importancia de elegir los mecanismos adecuados según las necesidades y características específicas de cada aplicación. Estos mecanismos deben estar alineados con el propósito de la investigación para contribuir al diseño y construcción de BC específicas para la CoC en evidencia digital, garantizando tanto la integridad como la trazabilidad de los datos.

3.3 Beneficios de BC para la CoC en evidencia digital en términos de integridad y trazabilidad (RQ2)

De acuerdo con los estudios seleccionados, se ilustra como BC ha revolucionado radicalmente la seguridad de la información al mejorar la auditabilidad, integridad, trazabilidad y confianza [61]. Esto resalta la importancia de continuar investigando en esta tecnología en el contexto de la CoC. La Tabla 8 resume los beneficios más significativos expuestos por los autores, relacionando las características de BC, que deben cumplir las aplicaciones destinadas al aseguramiento de la integridad y trazabilidad de las pruebas digitales en el proceso de la CoC [38], [51], [61].

Tabla 8
Beneficios de BC para la CoC en evidencia digital

Ref.	Beneficios	Auditabilidad	Credibilidad	Descentralización	Inmutabilidad	Integridad	Procedencia	Transparencia	Trazabilidad
[17], [43], [45]-[47], [49], [57]	Admisibilidad de la de evidencia digital.		√			√	√	√	
[44], [45] [47], [49], [51], [53]	Garantizar transparencia, confianza y autenticidad del proceso de CoC.		√				√	√	√

[42], [44]-[46], [49]-[51], [56], [57]	Mejorar la seguridad de las pruebas digitales.		√	√	√	√	√			
[17], [41], [47], [49], [51], [53]	Proporcionar trazabilidad de la evidencia digital.	√						√	√	

[17], [41]-[46], [49], [51], [54], [55], [57]	Preservar la integridad de la evidencia digital.			√		√	
[45]-[47], [49], [51], [53]	Auditabilidad del proceso de la CoC.	√				√	√

[17], [41]-[49], [51], [52], [55]-[57]	Registro de pruebas de forma segura.		√		√	√	
[42], [45], [48]-[51], [54], [56]	Verificar y validar accesibilidad de la evidencia digital.	√			√	√	√

Fuente: elaboración propia.

La marca de verificación (√) denota la descripción del beneficio de BC.

Se observa que la seguridad en el registro de pruebas y la preservación de la integridad de la evidencia digital son los temas más mencionados en los artículos, lo cual se alinea con la clasificación de las etapas de análisis forense expuestas en la Tabla 7. Esta relación destaca la relevancia de implementar soluciones basadas en BC que se ajusten a las etapas especificadas en la norma ISO/IEC 27037 [12], con el fin de fortalecer la seguridad y confiabilidad en el manejo de la evidencia digital en procedimientos forenses, y de esta manera contribuir a garantizar que las pruebas sean verificables y aceptadas en los estamentos judiciales. De igual forma, se refleja que las ocho características expuestas en las columnas, representan factores que siempre están presentes en las soluciones proporcionadas por BC debido a sus propiedades de inmutabilidad, integridad y trazabilidad [44], [46]. Estás características proporcionan confianza y fiabilidad al proceso de CoC, permitiendo así garantizar la procedencia de los datos y detectar cualquier posible intento de manipulación o acceso no autorizado a las pruebas digitales [47], [51], [53], requisitos esenciales para evitar la invalidez y rechazo de la evidencia digital en las investigaciones forenses.

3.4 Desafíos y limitaciones en la implementación de BC para la CoC en evidencia digital (RQ3)

En cuanto a los resultados obtenidos acerca de los desafíos en la implementación de la tecnología BC en el proceso de la CoC en evidencia digital, se encontró que existen varios retos planteados en los artículos revisados. La Tabla 9 presenta un resumen de esta información.

Tabla 9.
Desafíos de BC para la CoC en evidencia digital.

Ref.	Desafío	Descripción
[42], [46], [48], [52], [56]	Protección de datos	Por la naturaleza frágil, volátil, compleja y difusa de los datos, dan lugar a ser modificados o alterados con facilidad [42], [46]. Conservar la trazabilidad de las pruebas digitales representa un desafío considerable, dada la facilidad que resulta copiarlas, modificarlas o dañarlas [56]. Otro reto, es evitar la corrupción de las pruebas digitales en un sistema de preparación forense por parte de quienes las custodian [52]. Además, de mantener su integridad [48].
[42], [53]	Trazabilidad	Las pruebas digitales tienen la capacidad de ser copiadas y transferidas a otros sistemas, por lo cual se requiere el seguimiento constante del origen y el flujo de los datos relacionados con los casos [42], [53].
[42], [45], [52], [53]	Tipo y cantidad de datos	El creciente volumen de información digital y su heterogeneidad presenta un reto en términos de almacenamiento, procesamiento y análisis en los procesos de la CoC [42], [53]. De la misma forma, gestionar el incremento excesivo de información en la CoC, conocido como *blockchain bloat* [45]. Aparte de los desafíos asociados a la escalabilidad y multiarrendamiento para almacenamiento en la nube [52].
[17], [44]-[46], [49]	Regulación y cumplimiento normativo	El cumplimiento legal es un propósito importante, debido a la introducción de numerosas regulaciones y diversos modelos propuestos para el proceso de CoC [17], [44], [49]. Además, la falta de legalización dificulta el flujo de información entre las partes involucradas [46]. También, la oportunidad de definir estándares para los mecanismos de BC utilizados en la CoC [45].
[17], [53]	Privacidad de los datos	Mantener la confidencialidad de los datos en plataformas BC y sistemas en la nube, sin vulnerar la privacidad personal y pérdida de acceso a la información se considera un reto importante [17], [53].
[17], [43], [49], [52], [53]	Investigaciones nacionales y transfronterizas	Desarrollar plataformas de alcance global para asegurar la integridad de la CoC transjurisdiccional superando los desafíos derivados de la ubicación geográfica y multitenencia es un reto importante [17], [53]. Así mismo, mitigar los problemas asociados con la dispersión de los datos en la nube, los cuales pueden estar ubicados en distintas jurisdicciones [43], [52]. Además de facilitar el desarrollo ágil y sencillo de los procesos forenses a través de las fronteras jurisdiccionales [49].

Fuente: elaboración propia.

Estos retos describen importantes problemas que deben abordarse para aprovechar a su totalidad el potencial de la tecnología BC en el ámbito forense. Por lo tanto, la investigación debe centrar sus esfuerzos en resolver estos desafíos [62], [63], con el objetivo de proporcionar una visión más clara y completa sobre el panorama del tema de estudio. De esta manera, se puede generar nuevas propuestas de aplicación práctica que aseguren la fiabilidad, integridad y trazabilidad de las pruebas digitales [38].

Entre los hallazgos, se encuentra la importancia de la protección de datos [46], [52], especialmente la protección de información sensible y su prevención ante posibles vulnerabilidades. Así mismo, se resalta la necesidad del cumplimiento normativo [53], el cual es fundamental en el momento de validar la legitimidad del proceso en los tribunales de justicia. Otro reto importante, es la necesidad de contar con mecanismos, herramientas y normas para investigaciones nacionales y transfronterizas [49], [53]. Estos desafíos pueden ocasionar problemas de acceso a las pruebas, retrasos en el proceso y una baja confianza en la validación de la CoC. De igual forma, otros aspectos relacionados abarcan la trazabilidad, el tipo y cantidad de datos, así como la privacidad de la información. Estos factores son determinantes al momento de la adopción de BC como mecanismo para garantizar la integridad de la evidencia digital en las investigaciones forenses y su aceptación por parte de las partes interesadas. En cuanto a las limitaciones, se evidencia que BC a pesar de ser una tecnología disruptiva en el ámbito de la seguridad y con un futuro prometedor, todavía presenta vacíos importantes en el área de la ciencia forense. Por lo cual, requiere un mayor número de investigaciones para cerrar la brecha en la carencia de soluciones prácticas en el proceso de CoC en evidencia digital. En la Tabla 10 se hace una descripción detallada de las limitaciones abordadas en los estudios.

Tabla 10
Limitaciones de BC para la CoC en evidencia digital

Ref.	Limitación	Descripción
[52], [55]	Accesibilidad	La accesibilidad de los datos almacenados en la nube se encuentra limitada y depende de los permisos del proveedor y su cooperación con las investigaciones forenses. Por otra parte, la complejidad de las plataformas BC dificulta el acceso y uso de estos sistemas. Lo cual resulta en retrasos en el proceso CoC [52], [55].
[42], [53]	Almacenamiento	Almacenar grandes volúmenes de datos en BC se convierte en una operación poco eficiente, porque BC no fue diseñada para el almacenamiento de datos por su complejidad computacional para la ejecución de transacciones [42], [53].
[17]	Flexibilidad limitada	Los mecanismos de inmutabilidad de BC impiden en algunos casos cierto nivel de cambios en las transacciones del proceso de CoC que son necesarios en los procesos forenses, sin que afecte la legitimidad y autenticidad de las pruebas en el contexto legal [17].
[17], [44]	Formación en ciencia forense	La falta de profesionales con conocimientos en BC, representa una demanda de formación de todos los agentes implicados en la investigación forense en el ámbito jurídico como técnico. Esta carencia puede complicar la ejecución de la CoC y resultar en retrasos en los procesos judiciales [44]. Además de aumentar la brecha de investigación en tecnologías orientadas a la nube [17].
[56]	Interoperabilidad	La falta de estándares para la integración de plataformas y ecosistemas BC en diferentes entornos limitada la interoperabilidad entre los sistemas, lo cual conlleva a brechas en la seguridad de los datos, que puede ocasionar la inviabilidad del proceso de CoC para evidencia digital [56].
[17], [48], [53]	Marco jurídico y normativo	Los actuales marcos legales carecen de un proceso estándar y global que permita adoptar BC como mecanismo para el proceso de CoC en el manejo de evidencia digital, que garantice el cumplimiento de las leyes y sea válido en los tribunales [17], [48], [53].
[48], [54]	Multitenencia	En las investigaciones forenses, múltiples partes interesadas e intermediarios de confianza requieren acceder a las pruebas, existe el riesgo de que sean manipuladas. Esta situación dificulta la adaptación de los mecanismos de BC para preservar la integridad y seguridad de la evidencia digital [48], [54].
[17], [49]	Preservar registros digitales	Debido a su naturaleza, las evidencias o registros producidos por activos digitales en la nube son propiedad del proveedor. Esta particularidad implica que el registro de pruebas pueda ser borrado o eliminado. Además, los proveedores emplean sus propios formatos de registro que no siguen un estándar uniforme, lo cual aumenta el riesgo de contaminación o modificación de los registros durante su transferencia o almacenamiento [17], [49].

[17], [44]	Procedimientos forenses transfronterizos	La falta de claridad en la normatividad legal entre diversas jurisdicciones complica la gestión y la admisibilidad de las pruebas digitales en procedimientos judiciales [44]. Esta situación dificulta la cooperación y efectividad en la conducción de investigaciones forenses, aún más cuando las pruebas digitales se encuentran dispersas en distintas áreas geográficas, lo cual complica su acceso y utilización [17].
[47], [50], [51], [54]	Rendimiento	Las transacciones en BC se ven afectadas por la sobrecarga en los bloques, su tasa de crecimiento, la velocidad de procesamiento y la cantidad de participantes, que agrega latencia y limita su rendimiento. Lo cual impacta en el costo de despliegue de aplicaciones y recursos, que dificultad implementar nuevas BC [47], [50], [51], [54].
[17], [41], [42], [47], [52]	Seguridad en el proceso forense	La carencia de herramientas estándar o métodos eficientes para verificar e identificar vulnerabilidades de seguridad en procedimientos forenses en plataformas BC obstaculiza la capacidad de llevar a cabo servicios de auditoría y de mantener un seguimiento cronológico a las pruebas digitales. Esto conlleva a limitar la integridad y autenticidad de la CoC [17], [41], [42], [47], [52].

Fuente: elaboración propia.

En general, los autores proporcionan una base sólida de los desafíos y limitaciones que pueden orientar futuras investigaciones en BC para la CoC en evidencia digital y que es crucial abordar para avanzar en la aplicación de la tecnología BC en el análisis forense y así garantizar su utilidad en la preservación de la integridad y trazabilidad de la evidencia digital.

3.5 Perspectivas futuras y tendencias emergentes en la aplicación de BC para el proceso de CoC en evidencia digital (RQ4)

Aunque los resultados de la revisión de literatura acerca de BC y la CoC en evidencia digital, revelan que esta tecnología aún se encuentra en proceso de desarrollo, se observa un gran interés por investigar su aplicación en temas relacionados con la seguridad, privacidad, integridad y trazabilidad para la CoC en pruebas digitales, específicamente en el contexto forense y judicial, como se puede observar en el resumen presentado en la Tabla 11. Este interés se manifiesta en los estudios que presentan resultados prácticos, los cuales corresponden al 72,2 % de las investigaciones revisadas.

Tabla 11
Tendencias futuras para investigación

Ref.	Tendencia
[42]	Mejorar la escalabilidad de la CoC para el procesamiento de grandes volúmenes de datos.
[44], [53]	Aplicar leyes y normatividad vigente para en el uso de la tecnología BC en el proceso de la CoC a nivel global.
[43], [55]	Evaluar los parámetros de las plataformas y aplicaciones implementadas en BC para verificar y validar su funcionamiento adecuado y eficiente.
[42], [47]	Desarrollar sistemas y plataformas BC enfocadas en la interoperabilidad con otros sistemas y tecnologías empleadas en investigaciones forenses.
[52], [56]	Implementar sistemas forenses transfronterizos para la interacción multijurisdiccional en el proceso de CoC en evidencia digital.
[45], [52]	Construir aplicaciones BC para la CoC centradas en el manejo de datos almacenados en la nube.

Fuente: elaboración propia.

Entre los hallazgos se identificó que las tendencias para futuras investigaciones enmarcadas por los autores, se relacionan con iniciativas para el desarrollo de aplicaciones de BC enfocadas en mejorar la escalabilidad de la CoC para el manejo de grandes volúmenes de pruebas digitales [42]. También se hace referencia en la necesidad de aplicar la normatividad vigente para volver legítimo el uso de BC en el proceso de la CoC a nivel global [44], [53]. Además, se plantea la importancia de evaluar las plataformas y aplicaciones implementadas para verificar y validar su rendimiento, funcionalidad y costo [43], [55]. De igual forma, se sugiere la integración con otras tecnologías y entornos para mejorar la seguridad y la interoperabilidad de las aplicaciones y sistemas utilizados en investigaciones forenses [42], [47]. Así mismo, se describe la necesidad de implementar sistemas transfronterizos para casos que involucren múltiples jurisdicciones e interesados, lo cual permita un registro seguro y verificable de las pruebas en la CoC [52], [56]. Por último, se menciona el desarrollo de aplicaciones BC orientadas a datos almacenados en la nube [45], [52], como una respuesta ante la migración de sistemas y plataformas hacia este tipo de infraestructura. Estas direcciones de trabajos futuros identificadas en esta investigación reconocen el potencial de la tecnología BC como una herramienta con la capacidad de mejorar la seguridad, integridad y trazabilidad de la evidencia digital en los procesos forenses.

3.6 Discusión

En términos generales, es importante resaltar el notable crecimiento de la tecnología BC en los últimos años. Se puede observar el interés por el desarrollo de aplicaciones prácticas para la CoC en evidencia digital, con una tendencia a aumentar el número de investigaciones que podrían beneficiar a la ciencia forense en diferentes aspectos como autenticidad, confidencialidad, integridad y trazabilidad. La mayoría de estos estudios pueden representar un estímulo para motivar a otros investigadores a nivel global a iniciar sus proyectos encaminados en el uso de esta nueva tecnología. Esto se comprueba en los diferentes enfoques utilizados en los trabajos abordados, como se menciona en [42], [52], donde se destacan oportunidades de investigación para trabajar con BC y se enfatiza en la necesidad de desarrollar aplicaciones prácticas. Aunque, BC es una tecnología disruptiva que está siendo investigada en diferentes campos. Los hallazgos, resultado del SMS indican el

esfuerzo realizado por mejorar el proceso de la CoC, enfocándose en asegurar la integridad y el registro adecuado de las pruebas. Los autores presentan diferentes perspectivas para destacar las principales características que ofrece BC para asegurar el proceso de la CoC, con el fin garantizar la integridad y trazabilidad de la evidencia digital. Aunque los resultados presentados se encuentran sujetos al diseño metodológico, entorno de aplicación, plataforma de despliegue, tipo de datos y los registros almacenados en la BC, se evidencia que los estudios comparten características similares, lo cual permitió realizar una clasificación del estado actual de la adopción de la tecnología, centrándose en sus propiedades. Sin embargo, se observa algunas diferencias en la relevancia que cada autor define en algunos aspectos, lo cual revela diferentes enfoques y énfasis abordados en la literatura.

Para dar respuesta a la pregunta de investigación RQ1, se reconoce que se han identificado diferentes tipos de BC como privadas, públicas y autorizadas, que están siendo enmarcadas en dar solución a los problemas y desafíos de seguridad y manejo de datos digitales en la CoC. Entre estas, las plataformas Hyperledger y Ethereum se destacan debido a sus características inherentes, demostrando ser las más apropiadas para mantener la inmutabilidad, rastrear y proteger la integridad de los datos. Lo cual se ve reflejado en la clasificación de estudios prácticos realizados, como los mencionados en [43], [57]. En estos estudios, se afirma que estas plataformas son las más idóneas y cuentan con la infraestructura adecuada para la implementación de BC en entornos descentralizados distintos al de las criptomonedas, como se contrastó con nuestra revisión de literatura. Así mismo, se observa una evidente preferencia por plataformas BC que incorporan sistemas de autenticación obligatorio, que las convierte en sistemas más robustos y resistentes ante posibles vulneraciones y ataques. Esto confirma que la importancia en seguridad y autenticación es aún mayor en la protección de datos para entornos digitales, tal como ocurre en la preservación de la integridad y trazabilidad durante el proceso de CoC en evidencia digital.

En cuanto a la pregunta RQ2, es importante destacar las ventajas que los autores describen con relación al uso de BC, además de las propiedades y capacidades que esta tecnología ofrece para contribuir a diseñar y construir plataformas resistentes a manipulaciones y transparente a la hora de preservar las pruebas. En la Tabla 8 se ilustran estos beneficios, los cuales pueden servir como punto de referencia a otros investigadores interesados en comprender y aclarar las dudas acerca de las capacidades que ofrece BC en términos de confidencialidad, integridad, disponibilidad y trazabilidad, con el objetivo de mejorar los procesos de investigación forense. Otro aspecto para resaltar es la relación significativa entre integridad y trazabilidad. Esto se debe a que, al asegurar la integridad de las pruebas, automáticamente se cumple con el requisito de trazabilidad durante todo el proceso de CoC. De esta forma, la tecnología BC adquiere mayor relevancia como una herramienta que contribuye a fortalecer la inmutabilidad e integridad en el manejo de la evidencia digital.

Para la pregunta RQ3, se encuentra que la mayoría de las investigaciones revisadas, como [45], coinciden con los desafíos y limitaciones identificados en este mapeo de literatura. De igual forma, en otros trabajos mencionados, como en el caso de [38], también se encontró que estas dificultades son frecuentes en la implementación de aplicaciones y están relacionadas con el almacenamiento y la privacidad de los datos, el uso de plataformas en la nube, el diseño de aplicaciones para múltiples jurisdicciones y la trazabilidad de las pruebas. Estas dificultades evidencian las problemáticas que aún deben ser abordadas por la literatura, las cuales se corroboran con los hallazgos resultado de nuestro estudio. Por otra parte, es importante resaltar los esfuerzos realizados por los autores en sus trabajos por mejorar la seguridad, integridad y trazabilidad en el proceso de CoC para investigaciones forenses. Sin embargo, el avance tecnológico plantea nuevos desafíos, como la necesidad de adaptarse a nuevos enfoques, actualizar conocimientos y abordar la incertidumbre en cuanto a la normatividad legal, aspectos respaldados con la información obtenida en la literatura [45], [53]. Con la información extraída de los artículos se sintetizaron los resultados acercar de los retos que enfrenta el proceso de recolección de evidencia debido a los constantes cambios en el campo del análisis forense digital. Esto confirma que la capacidad de adaptación e innovación es esencial para garantizar la eficacia de los procesos de CoC en un entorno tecnológico en evolución. Para superar estos desafíos, se deben proponer soluciones

prácticas, impulsar la investigación y el desarrollo tecnológico. Esto permitirá estar a la vanguardia con los avances en el área de la seguridad informática, garantizando la disponibilidad de herramientas eficaces para el manejo de pruebas en casos legales, ofreciendo soluciones adecuadas al proceso de CoC en evidencia digital, para los nuevos vectores de ataques utilizados por los delincuentes digitales. Lo anterior, se ve reflejado en la presentación de 13 trabajos prácticos de los 18 trabajos finales seleccionados.

Para concluir, los resultados obtenidos en respuesta a la pregunta RQ4, representan una base fundamental para orientar la dirección de futuras investigaciones y proporcionar una perspectiva general del panorama actual sobre los beneficios y ventajas que la tecnología BC aporta a la seguridad de la CoC en evidencia digital, para garantizar su integridad y trazabilidad. Los hallazgos no solo contribuyen a una comprensión más profunda sobre la aplicación de BC en el ámbito forense, sino que también resaltan la importancia de seguir explorando nuevas posibilidades y aplicaciones de esta tecnología.

4. CONCLUSIONES

El SMS realizado identificó 18 estudios relevantes que permitieron extraer, analizar, comparar y discutir en profundidad sobre el rol que desempeña la tecnología BC para garantizar la integridad y trazabilidad en el contexto del proceso de CoC en evidencia digital. Basados en la revisión de estos estudios, se pudo destacar con claridad las fortalezas de la tecnología, evidenciadas por su capacidad única de garantizar la inmutabilidad, mantener la integridad y proporcionar trazabilidad a las pruebas digitales. Estas propiedades se resaltan como factores indispensables en el diseño y construcción de aplicaciones basadas en BC para el seguimiento confiable de la CoC en apoyo a investigaciones forenses. Por otra parte, se aprecia una estrecha relación entre la integridad y la trazabilidad en este contexto, ya que, al garantizar la integridad de cada registro almacenado en la BC, automáticamente se asegura la confiabilidad y autenticidad del proceso de auditoría que proporciona la trazabilidad. El cual es primordial para respaldar la confianza en la integridad de la evidencia digital y, a su vez, asegurar la fiabilidad y transparencia de todo el proceso de CoC.

Los resultados obtenidos permiten concluir que es fundamental continuar investigando en casos prácticos en entornos reales como una estrategia para hacer frente al desafío continuo que plantea el constante avance tecnológico en el ámbito de la seguridad informática digital. Es crucial comprender que el panorama actual de amenazas y vulnerabilidades se encuentra en constante evolución. Teniendo en cuenta que no existe un sistema completamente seguro y protegido de ataques externos, solo a través de la investigación continua y la aplicación práctica de soluciones innovadoras se puede hacer frente a este desafío. Esto es esencial para mantener la confianza, integridad y trazabilidad en los sistemas forenses digitales y en la CoC. También, se refleja la necesidad de desarrollar nuevos sistemas diseñados para investigaciones multijurisdiccionales que puedan ser utilizados por equipos multidisciplinares, los cuales sirvan como una solución integral para la recolección, almacenamiento, análisis y transmisión de pruebas transfronterizas, con capacidad de ser compatibles múltiples tecnologías. Esto permitirá afrontar las debilidades que presentan los sistemas forenses convencionales, tal como se señala en los estudios revisados. Por lo tanto, se espera que este estudio brinde un fundamento claro en la comprensión de la tecnología BC y su aplicación en el proceso de CoC, el cual permita fomentar un mayor interés y motivación para continuar investigando en esta área. De igual forma, es importante garantizar una formación y certificación constante en buenas prácticas para asegurar que el personal encargado de registrar, manipular y consultar las pruebas digitales en los procesos de investigación forense, mantenga la aplicación de los estándares y la normatividad vigente que permita la gestión correcta y segura de la CoC.

En un futuro cercano, y continuando con la evolución de la investigación en curso, se diseñará e implementará un mecanismo que utilice la tecnología BC como apoyo a fortalecer el proceso de CoC en el contexto de evidencia digital. Este mecanismo, servirá para verificar cada una de las etapas establecidas en la norma ISO/IEC 27037, que deben ser cumplidas en el proceso de informática forense. Además, ayudará a

validar y probar en un entorno de pruebas controlado con datos reales, los aspectos discutidos por los autores en sus estudios, con el fin de ayudar a contribuir en la mejora del ecosistema de la CoC y BC. También, se propondrá una metodología de alto nivel que sirva como referencia para la estandarización de los procedimientos de CoC mediante el uso BC, con el propósito de respaldar de manera completa todo el proceso forense y asegurar su aceptación por parte de todos los involucrados.

REFERENCIAS

[1] N. Rane, S. Choudhary, and J. Rane, "Enhanced Product Design and Development Using Artificial Intelligence (AI), Virtual Reality (VR), Augmented Reality (AR), 4D/5D/6D Printing, Internet of Things (IoT), and Blockchain: A Review," *SSRN Electron. J.*, Nov. 2023. http://dx.doi.org/10.2139/ssrn.4644059

[2] Sakshi, A. Malik, and A. K. Sharma, "Blockchain-based digital chain of custody multimedia evidence preservation framework for internet-of-things," *J. Inf. Secur. Appl.*, vol. 77, p. 103579, Sep. 2023. https://doi.org/10.1016/j.jisa.2023.103579

[3] W. Bank, "The Digital-Climate Nexus," In *Green Digital Transformation: How to Sustainably Close the Digital Divide and Harness Digital Tools for Climate Action*. Washington, DC: World Bank, 2023, pp. 1–23. https://openknowledge.worldbank.org/handle/10986/40653

[4] H. Koppisetty, K. Potdar, and S. Jain, "Cyber-crime, Forensics and use of Data Mining in Cyber Space: A Survey," in *2019 International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, 2019, pp. 722-727. https://doi.org/10.1109/ICSSIT46314.2019.8987921

[5] A. Musa Bade, and S. H. Othman, "Towards Adapting Metamodelling Technique for an Online Social Networks Forensic Investigation (OSNFI) Domain," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 7, 2022. http://dx.doi.org/10.14569/IJACSA.2022.0130722

[6] Á. MacDermott, T. Baker, P. Buck, F. Iqbal, and Q. Shi, "The Internet of Things: Challenges and Considerations for Cybercrime Investigations and Digital Forensics," *Int. J. Digit. Crime Forensics*, vol. 12, no. 1, pp. 1–13, Jan. 2020. http://doi.org/10.4018/IJDCF.2020010101

[7] A. Ombu, "Role of Digital Forensics in Combating Financial Crimes in the Computer Era," *J. Forensic Account. Prof.*, vol. 3, no. 1, pp. 57–75, Jun. 2023. https://doi.org/10.2478/jfap-2023-0003

[8] C. Chen, and B. Dong, "Digital forensics analysis based on cybercrime and the study of the rule of law in space governance," *Open Comput. Sci.*, vol. 13, no. 1, May. 2023. https://doi.org/10.1515/comp-2022-0266

[9] T. D'Anna *et al.*, "The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data," *Healthcare*, vol. 11, no. 5, p. 634, Feb. 2023. https://doi.org/10.3390/healthcare11050634

[10] A. A. Khan, M. Uddin, A. A. Shaikh, A. A. Laghari, and A. E. Rajput, "MF-Ledger: Blockchain Hyperledger Sawtooth-Enabled Novel and Secure Multimedia Chain of Custody Forensic Investigation Architecture," *IEEE Access*, vol. 9, pp. 103637–103650, Jul. 2021. https://doi.org/10.1109/ACCESS.2021.3099037

[11] T. M. jawad, "Adoption of Chain of Custody Improves Digital Forensic Investigation Process," *Iraqi J. Inf. Commun. Technol.*, vol. 1, no. 2, pp. 13–23, Jul. 2018. https://doi.org/10.31987/ijict.1.2.14

[12] *ISO/IEC 27037:2012 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence,* 27037:2012, ISO/IEC, Swiss, 2012. [Online]. Available: https://www.iso.org/standard/44381.html

[13] J. G. Nortjé, and D. C. Myburgh, "The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa," *Potchefstroom Electron. Law J.*, vol. 22, no. 1, pp. 1–42, Apr. 2019.

[14] N. M. Karie, V. R. Kebande, H. S. Venter, and K.-K. R. Choo, "On the importance of standardising the process of generating digital forensic reports," *Forensic Sci. Int. Reports*, vol. 1, p. 100008, Nov. 2019. https://doi.org/10.1016/j.fsir.2019.100008

[15] S. Li, T. Qin, and G. Min, "Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems," *IEEE Trans. Comput. Soc. Syst.*, vol. 6, no. 6, pp. 1433–1441, Dec. 2019. https://doi.org/10.1109/TCSS.2019.2927431

[16] G. Pestana, W. Antunes, and J. Carvalho, "Digital Chain of Custody Operational Framework," in *2023 IEEE International Workshop on Technologies for Defense and Security (TechDefense)*, Rome, Italy, 2023, pp. 417-422. https://doi.org/10.1109/TechDefense59795.2023.10380890

[17] K. Awuson-David, T. Al-Hadhrami, M. Alazab, N. Shah, and A. Shalaginov, "BCFL logging: An approach to acquire and preserve admissible digital forensics evidence in cloud ecosystem," *Futur. Gener. Comput. Syst.*, vol. 122, pp. 1–13, Sep. 2021. https://doi.org/10.1016/j.future.2021.03.001

[18] D. D. Pawlaszczyk, M. Bochmann, P. Engler, C. Klaver, and C. Hummert, "API-based evidence acquisition in the cloud - a survey [version 1; peer review: 1 approved, 1 approved with reservations]," *Open Res. Eur.*, vol. 2, no. 69, May. 2022. https://doi.org/10.12688/openreseurope.14784.1

[19] C. Karagiannis, and K. Vergidis, "Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal," *Information*, vol. 12, no. 5, p. 181, Apr. 2021.

[20] K. Mannix, A. Gorey, D. O'Shea, and T. Newe, "Sensor Network Environments: A Review of the Attacks and Trust Management Models for Securing Them," *J. Sens. Actuator Networks.*, vol. 11, no. 3, p. 43, Aug. 2022. https://doi.org/10.3390/jsan11030043

[21] M. Rasmi Al-Mousa, "Generic Proactive IoT Cybercrime Evidence Analysis Model for Digital Forensics," in *2021 International Conference on Information Technology (ICIT)*, Amman, Jordan, 2021, pp. 654-659. https://doi.org/10.1109/ICIT52682.2021.9491718

[22] T. D'Anna *et al.*, "The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data," *Healthcare*, vol. 11, no. 5, p. 634, Feb. 2023. https://doi.org/10.3390/healthcare11050634

[23] D. Banwani, and Y. Kalra, "Maintaining and Evaluating the Integrity of Digital Evidence in Chain of Custody," *Int. J. Recent Technol. Eng.*, vol. 10, no. 3, pp. 90–96, Sep. 2021. https://doi.org/10.35940/ijrte.c6449.0910321

[24] M. Li, C. Lal, M. Conti, and D. Hu, "LEChain: A blockchain-based lawful evidence management scheme for digital forensics," *Futur. Gener. Comput. Syst.*, vol. 115, pp. 406–420, Feb. 2021. https://doi.org/10.1016/j.future.2020.09.038

[25] O. Olukoya, "Distilling blockchain requirements for digital investigation platforms," *J. Inf. Secur. Appl.*, vol. 62, p. 102969, Nov. 2021. https://doi.org/10.1016/j.jisa.2021.102969

[26] S. K. Rana et al., "Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain," *IEEE Access*, vol. 11, pp. 83289–83300, Aug. 2023. https://doi.org/10.1109/ACCESS.2023.3302771

[27] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, Mar. 2008. https://bitcoin.org/bitcoin.pdf

[28] M. M. Khubrani, "Mobile Device Forensics, challenges and Blockchain-based Solution," in *2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, Singapore, 2023, pp. 1504-1509. https://doi.org/10.1109/SmartTechCon57526.2023.10391719

[29] S. Rao, S. Fernandes, S. Raorane, and S. Syed, "A Novel Approach for Digital Evidence Management Using Blockchain," in *Proc. Int. Conf. Recent Adv. Comput. Tech.*, Amsterdam, 2020, pp. 6. https://dx.doi.org/10.2139/ssrn.3683280

[30] P.A. Vaca, and E.R. Dulce-Villarreal, "El rol de la tecnología Blockchain para garantizar la integridad y trazabilidad al proceso de cadena de custodia: Un estudio de mapeo sistemático," in *Congreso Andino Computación, Informática y Educación - CACIED 2023,* 2023. [sin publicar]

[31] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic Mapping Studies in Software Engineering," in *12th Int. Conf. Eval. Assess. Softw.* Eng., Italy, 2008, pp. 1-10. https://doi.org/10.14236/ewic/EASE2008.8

[32] S.-M. Guerrero-Calvache, and G. Hernández, "Conceptions and Perceptions of Software Industry Professionals on Team Productivity in Agile Software Development: A Comparative Study," *Rev. Fac. Ing.*, vol. 30, no. 58, Dec. 2021. https://doi.org/10.19053/01211129.v30.n58.2021.13817

[33] M. Petticrew, and H. Roberts, "Starting the Review: Refining the Question and Defining the Boundaries," In *Systematic Reviews in the Social Sciences: A Practical Guide*. New York, NY, USA: Wiley, 2008, pp. 27–56. https://doi.org/10.1002/9780470754887

[34] B. Kitchenham, and S. M. Charters, "Guidelines for performing systematic literature reviews in software engineering," *University Durham, UK, Technical Report EBSE 2007-001. 2007.*https://docs.edtechhub.org/lib/EDAG684W

[35] T. Dyba, T. Dingsoyr, and G. K. Hanssen, "Applying Systematic Reviews to Diverse Study Types: An Experience Report," in *First International Symposium on Empirical Software Engineering and Measurement (ESEM 2007)*, Madrid, Spain, 2007, pp. 225-234. https://doi.org/10.1109/ESEM.2007.59

[36] T. Meline, "Selecting Studies for Systemic Review: Inclusion and Exclusion Criteria," *Contemp. Issues Commun. Sci. Disord.*, vol. 33, pp. 21–27, Mar. 2006. https://doi.org/10.1044/cicsd_33_S_21

[37] M. Guerrero-Calvache, and G. Hernández, Team Productivity in Agile Software Development: A Systematic Mapping Study, vol. 1643 CCIS. *Springer International Publishing*, 2022. https://dx.doi.org/10.1007/978-3-031-19647-8_32

[38] D. Batista et al., "Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review," *J. Risk Financ. Manag.*, vol. 16, no. 8, p. 360. 2023. https://doi.org/10.3390/jrfm16080360

[38] D. Batista et al., "Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review," *J. Risk Financ. Manag.*, vol. 16, no. 8, p. 360. 2023. https://doi.org/10.3390/jrfm16080360

[39] O. Revelo-Sánchez, C. A. Collazos-Ordoñez, and J. A. Jimenez-Toledo, "La Gamificación como estrategia didáctica para la enseñanza/aprendizaje de la programación: un mapeo sistemático de literatura," *Lámpsakos*, no. 19, pp. 31–46, Jan- Jun. 2018. https://doi.org/10.21501/21454086.2347

[40] E. R. D. Villarreal, J. García-Alonso, E. Moguel, and J. A. H. Alegría, "Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security," *IEEE Access*, vol. 11, pp. 5629–5652, Jan. 2023. https://doi.org/10.1109/ACCESS.2023.3236505

[41] W. Yan, J. Shen, Z. Cao, and X. Dong, "Blockchain Based Digital Evidence Chain of Custody," in *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology*, New York, NY, USA, 2020, pp. 19–23. https://doi.org/10.1145/3390566.3391690

[42] M. Ali, A. Ismail, H. Elgohary, S. Darwish, and S. Mesbah, "A Procedure for Tracing Chain of Custody in Digital Image Forensics: A Paradigm Based on Grey Hash and Blockchain," *Symmetry,* vol. 14, no. 2, p. 334, Feb. 2022. https://doi.org/10.3390/sym14020334

[43] L. Ahmad, S. Khanji, F. Iqbal, and F. Kamoun, "Blockchain-Based Chain of Custody: Towards Real-Time Tamper-Proof Evidence Management," in *Proceedings of the 15th International Conference on*

Availability, Reliability and Security, New York, NY, USA, 2020, pp. 1–8. https://doi.org/10.1145/3407023.3409199

[44] P. López-Aguilar, and A. Solanas, "An Effective Approach to the Cross-Border Exchange of Digital Evidence Using Blockchain," in *Applications in Electronics Pervading Industry, Environment and Society*, S. Saponara, A. de Gloria, Eds., Cham: Springer International Publishing, 2022, pp. 132–138. https://doi.org/10.1007/978-3-030-95498-7_19

[45] P. Santamaría, L. Tobarra, R. Pastor-Vargas, and A. Robles-Gómez, "Smart Contracts for Managing the Chain-of-Custody of Digital Evidence: A Practical Case of Study," *Smart Cities*, vol. 6, no. 2, pp. 709–727, Feb. 2023. https://doi.org/10.3390/smartcities6020034

[46] B. M. Manjre, and K. K. Goyal, "A novel and custom blockchain approach for the integrity assurance of the digital evidences extracted during the extraction and decoding of mobile artifacts from the mobile forensic tools," in *AIP Conference Proceedings*, Nagpur, India, 2023. https://doi.org/10.1063/5.0127910

[47] Sarishma, A. Gupta, and P. Mishra, "Blockchain based framework to maintain chain of custody (CoC) in a forensic investigation," in *Communications in Computer and Information Science*, M. Singh *et al.,* Eds., Cham: Springer International Publishing, 2021, pp. 37–46. https://doi.org/10.1007/978-3-030-81462-5_4

[48] M. Chopade, S. Khan, U. Shaikh, and R. Pawar, "Digital Forensics: Maintaining Chain of Custody Using Blockchain," in *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2019, pp. 744-747. https://doi.org/10.1109/I-SMAC47947.2019.9032693

[49] A. H. Lone, and R. N. Mir, "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer," *Digit. Investig.*, vol. 28, pp. 44–55, Mar. 2019. https://doi.org/10.1016/j.diin.2019.01.002

[50] Sunardi, and R. S. Kusuma, "Digital Evidence Security System Design Using Blockchain Technology," *Int. J. Saf. Secur. Eng.*, vol. 13, no. 1, pp. 159–165, Jan. 2023. https://doi.org/10.18280/ijsse.130118

[51] S. Bonomi, M. Casini, and C. Ciccotelli, "B-CoC: A blockchain-based chain of custody for evidences management in digital forensics," in *International Conference on Blockchain Economics, Security and Protocols (Tokenomics), Open Access Series in Informatics (OASIcs),* Paris, 2020, pp. 12:1-12:15. https://doi.org/10.4230/OASIcs.Tokenomics.2019.12

[52] O. W. Salami, M. B. Abdulrazaq, E. A. Adedokun, and B. Yahaya, "Collaborative Integrity Verification for Blockchain-Based Cloud Forensic Readiness Data Protection," in *Informatics and Intelligent Applications*, S. Misra, J. Oluranti, R. Damaševičius, and R. Maskeliunas, Cham: Springer International Publishing, 2022, pp. 138–152. https://doi.org/10.1007/978-3-030-95630-1_10

[53] H. Al-Khateeb, G. Epiphaniou, and H. Daly, "Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger," in *Advanced Sciences and Technologies for Security Applications*, H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, and H. Al-Khateeb, Eds., Cham: Springer International Publishing, 2019, pp. 149–168. https://doi.org/10.1007/978-3-030-11289-9_7

[54] T. Martin, and M. Hammoudeh, "Data Preservation System Using BoCA: Blockchain-of-Custody Application," in *The 5th International Conference on Future Networks & Distributed Systems*, New York, NY, USA, 2022, pp. 70–77. https://doi.org/10.1145/3508072.3508084

[55] A. Shahaab, C. Hewage, and I. Khan, "Preventing Spoliation of Evidence with Blockchain: A Perspective from South Asia," in *2021 The 3rd International Conference on Blockchain Technology*, New York, NY, USA, 2021, pp. 45–52. https://doi.org/10.1145/3460537.3460550

[56] X. Burri, E. Casey, T. Bollé, and D.-O. Jaquet-Chiffelle, "Chronological independently verifiable electronic chain of custody ledger using blockchain technology," *Forensic Sci. Int. Digit. Investig.*, vol. 33, p. 300976, Jun. 2020. https://doi.org/10.1016/j.fsidi.2020.300976

[57] T. Fu-Ching, "The application of blockchain of custody in criminal investigation process," *Procedia Computer Science*, vol. 192, pp. 2779–2788, 2021. https://doi.org/10.1016/j.procs.2021.09.048

[58] E. Dulce, and J. Hurtado, "The Role of the Blockchain Technology in the Elderly Care Solutions: A Systematic Mapping Study," in *Gerontechnology III*, J. García-Alonso, and C. Fonseca, Eds., Cham: Springer International Publishing, 2021, pp. 23–34. https://doi.org/10.1007/978-3-030-72567-9_3

[59] J. Chen, X. Xia, D. Lo, J. Grundy, and X. Yang, "Maintaining Smart Contracts on Ethereum: Issues, Techniques, and Future Challenges," 2021. https://doi.org/10.48550/arXiv.2007.00286

[60] V. Dhillon, D. Metcalf, and M. Hooper, "The Hyperledger Project," in *Blockchain Enabled Appl.*, Berkeley, CA: Apress, 2017, pp. 139–149. https://doi.org/10.1007/978-1-4842-3081-7_10

[61] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing," *Futur. Internet*, vol. 14, no. 11, p. 341, Nov. 2022. https://doi.org/10.3390/fi14110341

[62] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, Oct. 2018. http://dx.doi.org/10.1504/IJWGS.2018.095647

[63] W. Gao, W. G. Hatcher, and W. Yu, "A Survey of Blockchain: Techniques, Applications, and Challenges," in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, Hangzhou, China, 2018, pp. 1-11. https://doi.org/10.1109/ICCCN.2018.8487348

Notas

5. AGRADECIMIENTO Y FINANCIACIÓN:
Este trabajo no cuenta con apoyo económico de ninguna entidad. Se agradece a la Universidad de Nariño y Universidad Nacional Abierta y a Distancia por su apoyo en el acceso a material bibliográfico.

CONFLICTOS DE INTERÉS DE LOS AUTORES :
No existe entre los autores conflictos de intereses de tipo financiero, profesional o personal, que hubieran podido afectar de manera directa en el desarrollo de la presente revisión.

CONTRIBUCIÓN DE LOS AUTORES :
Tanto la concepción como la redacción y análisis de la información fue realizada de manera conjunta por los autores.
Los aportes específicos consistieron en:
- *Pablo A. Vaca*, contribuyó en la conceptualización, metodología, investigación, redacción, revisión y edición.
- *Edgar R. Dulce-Villarreal*, contribuyó en la metodología, investigación, redacción, revisión y edición.

Información adicional

Cómo citar / How to cite: P. A. Vaca, and E. R. Dulce-Villarreal, "Blockchain para asegurar la integridad y trazabilidad en la cadena de custodia de evidencia digital en informática forense: un estudio de mapeo sistemático," *TecnoLógicas*, vol. 27, no. 60, e3049, jul. 2024. https://doi.org/10.22430/22565337.3049

Enlace alternativo

https://revistas.itm.edu.co/index.php/tecnologicas/issue/view/138 (html)

Pablo A. Vaca, Edgar R. Dulce-Villarreal

Blockchain para asegurar la integridad y trazabilidad en la cadena de custodia de evidencia digital en informática forense: un estudio de mapeo sistemático

Blockchain for Ensuring Integrity and Traceability in the Chain of Custody of Digital Evidence in Computer Forensics: A Systematic Mapping Study

TecnoLógicas
vol. 27, núm. 60, p. 1 - 25, 2024
Instituto Tecnológico Metropolitano, Colombia
tecnologicas@itm.edu.co

ISSN: 0123-7799 **/ ISSN-E:** 2256-5337

DOI: https://doi.org/10.22430/22565337.3049