Cadena de Custodia: Evaluando Soluciones Blockchain bajo la Norma ISO 27037

Conference Paper · April 2025

DOI: 10.5281/zenodo.15210331

2 authors:

Irene Lavín
University of Valladolid
4 PUBLICATIONS **1** CITATION
SEE PROFILE

Diego R. Llanos
University of Valladolid
164 PUBLICATIONS **959** CITATIONS
SEE PROFILE

Cadena de Custodia: Evaluando Soluciones Blockchain bajo la Norma ISO 27037

Chain of Custody: Evaluating Blockchain Solutions under ISO 27037

Irene Lavín
Universidad de Valladolid
Valladolid, España
irene.lavin@uva.es

Diego R. Llanos
Universidad de Valladolid
Valladolid, España
diego.llanos@uva.es

Resumen —**La preservación de la cadena de custodia (CdC) es esencial para garantizar la integridad y autenticidad de la evidencia digital en entornos legales y forenses. Este artículo examina cómo las soluciones basadas en Blockchain abordan los requisitos de la norma ISO 27037, que regula la identificación, recolección, adquisición y preservación de evidencia digital. El análisis revela importantes deficiencias en aspectos como auditabilidad, escalabilidad y admisibilidad legal. Finalmente, se presentan recomendaciones clave para fortalecer la integración entre Blockchain y las directrices de la ISO 27037, fomentando soluciones más robustas y alineadas con los estándares forenses internacionales.**

Palabras Clave - ISO 27037; CdC; blockchain.

Abstract — **Chain of custody (CoC) preservation is essential to ensure the integrity and authenticity of digital evidence in legal and forensic settings. This article examines how Blockchain-based solutions address the requirements of ISO 27037, which regulates the identification, collection, acquisition and preservation of digital evidence. The analysis reveals significant shortcomings in aspects such as auditability, scalability and legal admissibility. Finally, key recommendations are presented to strengthen the integration between Blockchain and ISO 27037 guidelines, fostering more robust solutions aligned with international forensic standards.**

Keywords - ISO 27037; CoC; blockchain.

I. INTRODUCCIÓN

En un mundo cada vez más digital, preservar la cadena de custodia de los activos digitales es crucial para garantizar la integridad y procedencia de los datos. Este artículo tiene como objetivo explorar las soluciones existentes basadas en la tecnología Blockchain para mejorar la cadena de custodia de los activos digitales y analizar, centrándose en la norma ISO 27037 [1], si dichas soluciones integran la norma. Esto proporcionaría una comprensión integral del estado actual del arte, identificaría las fortalezas y limitaciones de los enfoques existentes y guiaría la futura investigación y desarrollo en este campo.

La norma ISO 27037, que proporciona directrices para el manejo de evidencia digital, puede verse fortalecida por la tecnología Blockchain. La naturaleza descentralizada, inmutable y transparente de Blockchain permite la preservación automática de datos, creando una cadena de custodia segura y auditable [2]. Investigaciones previas como Forensic-Chain [3] y B-DEC [4] han demostrado el potencial de soluciones basadas en Blockchain para mejorar la gestión de evidencia digital. Además, la aplicación de Blockchain en la gestión de datos personales destaca su capacidad para mejorar la auditabilidad y transparencia en la recopilación, retención e intercambio de datos [5].

II. ANÁLISIS DE LA NORMA ISO 27037

La norma ISO 27037 proporciona un marco integral para la gestión de evidencias digitales, que abarca la identificación, recogida, adquisición y preservación [6]. Detalla los pasos esenciales para garantizar la integridad y admisibilidad de la evidencia digital en procesos legales, destacando la documentación de la cadena de custodia.

Específicamente, la norma enfatiza la importancia de mantener una cadena de custodia clara e ininterrumpida, lo que implica documentar la posesión, el manejo y el control de la evidencia digital desde su identificación inicial hasta su disposición final [7]. Este proceso es crucial para establecer la autenticidad y la confiabilidad demostrando que la evidencia no ha sido manipulada ni alterada durante la investigación. La norma también aborda el almacenamiento seguro, la conservación del estado original de las pruebas [8] y el mantenimiento de registros detallados a lo largo de toda la cadena de custodia [9].

A. Propósito y Alcance

La norma ISO 27037 sirve como guía para las organizaciones y personas involucradas en el manejo de evidencia digital, como agencias de aplicación de la ley, investigadores forenses y profesionales de seguridad de la información.

Los tres objetivos principales de la norma [1] son:

- Identificación, recogida, adquisición y preservación de evidencia digital.

- Asegurar la integridad de la evidencia para acciones legales, disciplinarias o de investigación.
- Facilitar el intercambio de evidencia digital entre jurisdicciones.

Se aplica a múltiples dispositivos, incluyendo ordenadores, discos duros, teléfonos móviles y sistemas en red. Cámaras digitales fijas y de vídeo, sistemas de navegación y dispositivos similares.

B. Principios Clave

La norma ISO 27037 destaca varios principios clave [1] que son esenciales para preservar la cadena de custodia de la evidencia digital:

- Relevancia: La evidencia debe estar directamente relacionada con la investigación.
- Confiabilidad: Los procesos deben asegurar que la evidencia es lo que dice ser.
- Suficiencia: Se debe recoger evidencia adecuada para apoyar la investigación.

Además, la norma enfatiza la importancia de mantener el estado original de la evidencia, prevenir la contaminación y asegurar procedimientos de manejo estrictos.

C. Manejo de Evidencia Digital

1) Aspectos clave del Manejo de Evidencia Digital

Varios aspectos clave que son cruciales para el manejo efectivo de la evidencia digital son subrayados por la norma ISO 27037 [1]. Estos elementos centrales, como se describe en la norma, incluyen:

- Auditabilidad: Registro completo y transparente de todas las acciones sobre la evidencia digital, facilitando su verificación independiente.
- Justificabilidad: Una justificación clara para todas las decisiones y acciones tomadas durante el proceso de manejo de la evidencia.
- Repetibilidad: La capacidad de obtener los mismos resultados cuando el mismo proceso es seguido por una persona diferente utilizando las mismas herramientas y métodos bajo las mismas condiciones.
- Reproducibilidad: La capacidad de obtener los mismos resultados cuando el mismo proceso es seguido por una persona diferente utilizando diferentes herramientas y métodos bajo diferentes condiciones.

2) Procesos para el Manejo de Evidencia Digital

La norma ISO 27037 describe una serie de procesos para el manejo de evidencia digital [1]. Estos procesos son críticos para establecer la integridad y la trazabilidad de la evidencia digital, lo cual es esencial para su admisibilidad en procedimientos legales. Los métodos se describen a continuación.

- Identificación: Reconocer y documentar la evidencia digital potencial, priorizando la recolección basada en la volatilidad de los datos para evitar su pérdida.
- Recolección: Trasladar los dispositivos que contienen evidencia digital a instalaciones seguras para su examen. Documentar exhaustivamente todas las acciones emprendidas.
- Adquisición: Crear copias verificadas de la evidencia digital utilizando métodos y herramientas aprobados.
- Preservación: La evidencia debe protegerse de la manipulación, los peligros ambientales y los daños accidentales. Debe almacenarse en instalaciones seguras con controles de acceso y monitoreo.

D. Asegurando la exactitud e integridad de la Evidencia Digital

La norma ISO 27037 [1] enfatiza la importancia de mantener la exactitud e integridad de la evidencia digital durante todo el proceso de investigación. Esto asegura que la copia de la evidencia sea correcta y no haya sido manipulada. Se utiliza una combinación de salvaguardias técnicas y de procedimiento de la siguiente manera.

- Uso de Funciones de Verificación: Demostrar que la evidencia no ha sido modificada.
- Cadena de Custodia: Detalla los requisitos para mantener un registro de la cadena de custodia.
- Repetibilidad y Reproducibilidad: Todos los procesos deben ser *auditables y repetibles* y sus resultados *reproducibles*.
- Intrusión Mínima: Tratar de minimizar los cambios en los datos originales.
- Documentación y Validación: Documentar todas las acciones y establecer un método para verificar la exactitud y la confiabilidad de las copias en comparación con el original.
- Manejo de Datos Volátiles: Directrices específicas para el manejo de datos volátiles debido a su susceptibilidad a la pérdida.
- Uso de Herramientas Confiables y Bloqueadores de Escritura: El uso de bloqueadores de escritura está implícito en el énfasis en minimizar los cambios en los datos originales.
- Registro y Rastros de Auditoría: Menciona la importancia de *auditar y justificar*.

E. Roles y Responsabilidades

ISO 27037 [1] solo menciona como tales dos roles principales, la Primera Respuesta de Evidencia Digital (DEFR) y el Especialista en Evidencia Digital (DES). Sin embargo, implícitamente define varios roles clave. Estos roles, Custodiador de Evidencia Digital (DEC), Autoridad Legal (LA) y Gestión de Instalaciones Forenses (FFM), emergen de las actividades descritas dentro de la norma.

La Tabla I muestra un resumen de las responsabilidades deducidas para cada rol presentado anteriormente.

TABLA I. RESUMEN DE LAS RESPONSABILIDADES DEDUCIDAS DE LOS ROLES DE LA NORMA ISO 27037

- **Primera Respuesta de Evidencia Digital (DEFR)**
  - Asegurar la escena: Proteger la ubicación y los dispositivos del acceso o alteración no autorizados.
  - Identificar evidencia potencial: Reconocer los dispositivos que pueden contener información digital relevante.
  - Documentar el estado inicial: Tomar notas, fotos o videos antes de tocar o mover cualquier evidencia.
  - Prevenir la alteración de datos: Evitar acciones que puedan modificar los datos.
  - Informar los hallazgos a las autoridades o especialistas.
- **Especialista en Evidencia Digital (DES)**
  - Identificación de evidencias digital relevantes.
  - Recolección de dispositivos físicos y medios de manera forense y sólida.
  - Adquisición de copias forenses para asegurar la integridad y prevenir la alteración.
  - Preservación de la evidencia digital durante todo su ciclo de vida, almacenamiento y la cadena de custodia.
  - Documentación meticulosa de todas las acciones para mantener la auditabilidad y la cadena de custodia.
  - Cumplimiento de los requisitos legales y organizacionales.
- **Custodiador de Evidencia Digital (DEC)**
  - Mantener la cadena de custodia: Documentar todos los aspectos de evidencia, fechas de transferencia y razones.
  - Almacenamiento seguro: Proteger la evidencia del acceso no autorizado, daños o degradación.
  - Acceso controlado: Restringir quién puede acceder a la evidencia, con registros de acceso.
  - Manejo adecuado: Transferir la evidencia según los procedimientos y documentar en la cadena de custodia.
- **Autoridad Legal (LA)**
  - Iniciar la investigación y la necesidad de evidencia digital.
  - Definir el alcance de la investigación y la evidencia digital requerida.
  - Proporcionar autorización legal para la recolección y adquisición de evidencia.
  - Recibir informes y hallazgos del examen de evidencia digital.
  - Asegurar la conducta legal y ética de la investigación.
- **Gestión de Instalaciones Forenses (FFM)**
  - Alinear los procedimientos con la norma ISO 27037.
  - Asegurar que el personal esté capacitado y sea competente en el manejo de evidencia digital.
  - Proporcionar las herramientas y recursos necesarios para el trabajo forense digital.
  - Supervisar los procesos de control de calidad/aseguramiento de la calidad en el laboratorio.
  - Gestionar el flujo de trabajo y los recursos para las investigaciones digitales.

F. Competencia y Capacitación

La norma [1] enfatiza la importancia de una capacitación y certificación adecuadas para todo el personal involucrado en el proceso de manejo de evidencia digital. Se definen requisitos de competencia para cada uno de los roles clave, asegurando que las personas tengan las habilidades y el conocimiento necesarios para cumplir con sus responsabilidades manteniendo la integridad de la evidencia.

G. Directrices Adicionales

Esta sección de la norma ISO 27037 [1] describe orientación complementaria sobre aspectos cruciales de la manipulación de pruebas digitales, haciendo hincapié en la documentación adecuada, la puesta al día y el cumplimiento de los requisitos legales. Estas directrices adicionales proporcionan un enfoque más holístico de la gestión de pruebas digitales, en consonancia con los principios y requisitos de la norma.

III. SOLUCIONES BASADAS EN BLOCKCHAIN Y LA NORMA ISO 27037

A continuación, examinaremos varias soluciones existentes e investigaciones relacionadas con la aplicación de Blockchain al tratamiento de la cadena de custodia y la evidencia digital. El objetivo es ver si tienen en cuenta la norma ISO 27037 en su investigación, así como determinar hasta qué grado y cuáles son las posibles áreas de mejora.

Las Tablas II y III muestran un resumen de soluciones basadas en Blockchain, así como un análisis de la cobertura de la norma ISO 27037 y las áreas de mejora detectadas.

IV. RESUMEN DE CARACTERÍSTICAS FALTANTES

En la Tabla IV se exponen una condensación de características faltantes en los artículos sometidos a análisis. Tal y como se puede observar, las áreas de mejora se agrupan en tres bloques: la correspondencia con la ISO 27037, la implementación práctica y escalabilidad y la admisibilidad legal e integración. Para cada una de las soluciones analizadas se ha marcado con un aspa (×) el área de mejora. Algunos de los trabajos se centran en un análisis y no proveen una solución como tal. En estos casos, se ha revisado igualmente si ofrecen una cobertura de la norma ISO 27037, si detallan una posible guía para una futura solución y si tienen en cuenta un análisis en torno a la admisibilidad legal.

V. CONCLUSIONES

En relación con las áreas de mejora concentradas en la Tabla IV, se observa que el 100% de las soluciones analizadas no establecen una correspondencia clara con las cláusulas específicas de la norma ISO 27037 ni demuestran explícitamente cómo cumplir los cuatro principios clave de la norma (auditabilidad, justificabilidad, repetibilidad y reproducibilidad). Asimismo, un 33,3% de los trabajos revisados no abordan suficientemente la implementación práctica. Tampoco la escalabilidad de las soluciones propuestas, con un 41,6%, obviando aspectos cruciales como la

TABLA II. RESUMEN DE SOLUCIONES BASADAS EN BLOCKCHAIN INDICANDO LA COBERTURA DE LA NOMRA ISO 27037 Y LAS ÁREAS DE MEJORA DETECTADAS (PRIMERA PARTE)

1. *B-CoC: A Blockchain-Based Chain of Custody for Evidence Management in Digital Forensics* [10]
   - **Cobertura**: Este artículo propone un sistema basado en Blockchain para desmaterializar el proceso de CdC, asegurando la integridad y la trazabilidad de la evidencia recolectada. Incluye una implementación prototipo utilizando Ethereum y evalúa su rendimiento.
   - **Áreas de mejora**:
     - Hay una discusión limitada sobre la integración de soluciones Blockchain con los estándares ISO existentes como ISO 27037.
     - No proporciona una taxonomía integral de las soluciones de CdC basadas en Blockchain.
     - Carece de exploración de la admisibilidad legal y los desafíos entre jurisdicciones.
2. *A Survey on Blockchain-Based IoT Forensic Evidence Preservation* [11]
   - **Cobertura**: Esta revisión examina el papel de Blockchain en la preservación de evidencia forense dentro de entornos de IoT, abordando desafíos como la integridad y autenticidad de la evidencia.
   - **Áreas de mejora**:
     - Se centra principalmente en contextos de IoT, con menos énfasis en la CdC de activos digitales más amplia.
     - No analiza las normas ISO ni establece una taxonomía detallada de las soluciones de Blockchain.
     - Hay una discusión limitada sobre la auditabilidad de los hashes recolectados.
3. *Exploring Blockchain Technology for Chain of Custody Control in Physical and Digital Evidence* [12]
   - **Cobertura**: A través de una revisión sistemática de la literatura, este artículo analiza las soluciones basadas en Blockchain para los problemas de CdC aplicables tanto a la evidencia física como a la digital.
   - **Áreas de mejora**:
     - No profundiza en el análisis de la norma ISO 27037.
     - Carece de una taxonomía estructurada de las soluciones de CdC basadas en Blockchain.
     - Hay un enfoque mínimo en los aspectos de auditabilidad de los hashes recolectados.
4. *Blockchain para asegurar la integridad y trazabilidad en la cadena de custodia de la evidencia digital* [13]
   - **Cobertura**: Esta investigación clasifica las características de Blockchain que aseguran la integridad y la trazabilidad de la evidencia digital en el proceso de CdC basándose en un estudio de mapeo sistemático.
   - **Áreas de mejora**:
     - Análisis limitado de las normas ISO.
     - No proporciona una taxonomía integral de las soluciones de Blockchain.
     - Carece de discusión sobre la auditabilidad de los hashes recolectados.
5. *ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability* [14]
   - **Cobertura**: Este artículo presenta un marco de Blockchain que automatiza los pasos de la investigación, asegura el acceso seguro a los datos, rastrea los orígenes de los datos, preserva los registros y acelera la extracción de la procedencia.
   - **Áreas de mejora**:
     - No analiza la norma ISO 27037 ni las normas relacionadas.
     - Carece de una taxonomía detallada de las soluciones de CdC basadas en Blockchain.
     - Se centra más en la procedencia y la auditabilidad que en todo el proceso de CdC.
6. *B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management* [4]
   - **Cobertura**: B-DEC, una solución basada en Blockchain, aborda directamente los aspectos centrales de la gestión de evidencia digital descritos en la norma ISO 27037. Proporciona un sistema seguro y auditable para registrar los detalles de la evidencia, los registros de acceso y la información de la cadena de custodia.
   - **Áreas de mejora**:
     - No demuestra cumplimiento con los cuatro aspectos clave del manejo de evidencia digital definidos en la norma.
     - Centrado en la implementación técnica de B-DEC, sin apoyarse en la norma ISO 27037.
     - Proporciona detalles limitados sobre cómo se aseguran la auditabilidad y la integridad de los hashes registrados.
7. *Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions* [15]
   - **Cobertura**: Proporciona una amplia descripción general de la informática forense de Blockchain, que abarca técnicas, aplicaciones y desafíos. También abordan los desafíos forenses clave relacionados con la integridad, autenticidad y no repudio de los datos.
   - **Áreas de mejora**:
     - Carece de una discusión sobre cómo la informática forense de Blockchain se alinea con los requisitos de la norma ISO 27037.
     - No proporciona un mapeo entre las técnicas discutidas y secciones de la norma ISO 27037.
     - Se centra en los aspectos teóricos y técnicos de la informática forense de Blockchain, sin discusión sobre la implementación práctica.

TABLA III. RESUMEN DE SOLUCIONES BASADAS EN BLOCKCHAIN INDICANDO LA COBERTURA DE LA NOMRA ISO 27037 Y LAS ÁREAS DE MEJORA DETECTADAS (SEGUNDA PARTE)

8. *A Data Preservation Method Based on Blockchain and Multidimensional Hash for Digital Forensics* [2]
   - **Cobertura**: El método propuesto utiliza Blockchain y hashing multidimensional para asegurar la integridad de los datos. La técnica de hashing multidimensional contribuye a asegurar la autenticidad y verificabilidad de la evidencia preservada.
   - **Áreas de mejora**:
     - Carece de referencia explícita y alineación con la norma ISO 27037.
     - Análisis limitado de cómo el método se integra con los procesos y directrices generales descritos en la norma ISO 27037.
     - Detalles insuficientes sobre la implementación práctica y la escalabilidad del método propuesto.
     - No se describen las implicaciones legales con respecto a la admisibilidad de la evidencia basada en Blockchain en los tribunales.
9. *Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer* [3]
   - **Cobertura**: Forensic-chain, una solución basada en Blockchain, aborda directamente la cadena de custodia. Tiene como objetivo crear un registro seguro y a prueba de manipulaciones del manejo de la evidencia, demostrando una implementación práctica con una Prueba de Concepto utilizando Hyperledger Composer.
   - **Áreas de mejora**:
     - No se apoya en la norma y carece de una demostración clara de cómo cumple con sus requisitos.
     - Se centra en un caso de uso específico y no aborda el contexto más amplio de la norma o la integración con otros procesos forenses.
     - No discute las implicaciones legales del uso de evidencia basada en Blockchain, particularmente en lo que respecta a su admisibilidad en los tribunales.
10. *Blockchain Based Digital Evidence Chain of Custody* [6]
    - **Cobertura**: La solución propuesta aprovecha la tecnología Blockchain para crear un registro a prueba de manipulaciones y transparente del manejo de la evidencia. Incorpora mecanismos de marca de tiempo para proporcionar registros verificables de la adquisición y el manejo de la evidencia.
    - **Áreas de mejora**:
      - Carece de una demostración clara de cómo cumple con los requisitos de la norma.
      - No proporciona detalles suficientes sobre la implementación práctica y la escalabilidad de la solución propuesta.
      - No discute las implicaciones legales del uso de evidencia basada en Blockchain.
11. *Blockchain-based chain of custody* [9]
    - **Cobertura**: Blockchain mejora la confiabilidad de la cadena de custodia al proporcionar un registro a prueba de manipulaciones, transparente y auditable del manejo de evidencia digital.
    - **Áreas de mejora**:
      - Carece de una demostración clara de cómo la solución cumple con los requisitos de la norma.
      - No proporciona detalles sobre la implementación práctica y la escalabilidad.
      - No discute las implicaciones legales del uso de evidencia basada en Blockchain o cómo la solución se integra con los procesos y herramientas forenses existentes.
12. *SoK: Blockchain Solutions for Forensics* [16]
    - **Cobertura**: Este artículo de sistematización del conocimiento examina varias soluciones de Blockchain para forenses, incluyendo su potencial para mejorar la cadena de custodia. Proporciona una descripción general completa de diferentes enfoques y sus fortalezas y debilidades.
    - **Áreas de mejora**:
      - No propone una solución específica.
      - No aborda directamente los requisitos de la norma ISO 27037 ni los detalles de implementación.

integración con sistemas existentes, la gestión de grandes volúmenes de datos y la interoperabilidad entre distintas plataformas. La falta de claridad sobre el rendimiento y eficacia de las soluciones en la práctica se ha contabilizado en el 83,3% de los casos. Finalmente, la admisibilidad legal de la evidencia almacenada en Blockchain, un aspecto fundamental para su utilización en procesos judiciales, también se encuentra escasamente tratada en la literatura revisada, solo en un 16,7% de los casos. Estas carencias representan un obstáculo para la adopción generalizada de la tecnología Blockchain en la gestión de la cadena de custodia de evidencia digital.

Como trabajo futuro y, para fortalecer la integración entre Blockchain y la norma, propondremos una taxonomía exhaustiva que clasifique las soluciones basadas en Blockchain para la cadena de custodia según criterios como el tipo de Blockchain (pública, privada, híbrida), mecanismos de consenso, arquitectura de almacenamiento, escalabilidad e integración con la norma ISO 27037.

TABLA IV. SUMARIO DE CARACTERÍSTICAS FALTANTES EN LAS SOLUCIONES ANALIZADAS.

	Bonomi et al. [10]	Sakshi et al. [11]	Batista et al. [12]	Vaca et al. [13]	Akbarfam et al. [14]	Yunianto et al. [4]	Atlam et al. [15]	Liu et al. [2]	Lone et al. [3]	Wenqi et al. [6]	Ahmad et al. [9]	Dasaklis et al. [16]
Correspondencia explícita con ISO 27037												
Falta correspondencia clara y detallada de las cláusulas específicas de la norma que cubre la solución.	×	×	×	×	×	×	×	×	×	×	×	×
Falta demostración explícita de cómo se cumplen los cuatro principios clave de la norma.	×	×	×	×	×	×	×	×	×	×	×	×
Implementación práctica y escalabilidad												
Detalle insuficiente sobre aplicación práctica de la solución.			×				×	×				×
Información limitada sobre escalabilidad de la solución.			×				×	×		×	×	
Falta claridad sobre rendimiento y eficacia de las soluciones en la práctica.	×		×	×	×	×	×	×	×	×	×	
Admisibilidad legal e integración												
Insuficiente debate sobre las implicaciones jurídicas del uso de pruebas basadas en Blockchain.	×	×		×	×	×	×	×	×	×	×	
Análisis insuficiente de cómo se integran con los marcos jurídicos y procedimientos probatorios.	×	×	×	×	×	×	×	×	×	×	×	×

AGRADECIMIENTOS

El presente trabajo ha sido financiado en parte por el proyecto NATASHA (PID2022-142292NB-I00), del Ministerio de Ciencia, Innovación y Universidades de España.

REFERENCIAS

[1] ISO/IEC, "ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence". International Organization for Standardization, 2012.

[2] G. Liu, J. He, and X. Xuan, "A Data Preservation Method Based on Blockchain and Multidimensional Hash for Digital Forensics", *Complexity*, vol. 2021, no. 1, Jan. 2021.

[3] A. H. Lone and R. N. Mir, "Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer", *Digital Investigation*, vol. 28, pp. 44–55, Mar. 2019.

[4] E. Yunianto, Y. Prayudi, and B. Sugiantoro, "B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management", *IJCA*, vol. 181, no. 45, pp. 22–29, Mar. 2019.

[5] A. Masluk and M. Gofman, "Protecting Personal Data with Blockchain Technology", in *Information Technology - New Generations*, S. Latifi, Ed., Cham: Springer International Publishing, 2018, pp. 119–125.

[6] W. Yan, J. Shen, Z. Cao, and X. Dong, "Blockchain Based Digital Evidence Chain of Custody", in *Proceedings of the 2020 2nd International Conference on Blockchain Technology*, Hilo HI USA: ACM, Mar. 2020, pp. 19–23.

[7] V. Wylde *et al.*, "Cybersecurity, Data Privacy and Blockchain: A Review", *Springer Nature*, vol. 3, no. 2. Jan. 2022.

[8] M. D. Sheldon, "Tracking Tangible Asset Ownership and Provenance with Blockchain". American Accounting Association vol. 36, no. 3, pp. 153–175, Apr. 2022.

[9] 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*, Virtual Event Ireland: ACM, Aug. 2020, pp. 1–8.

[10] S. Bonomi, M. Casini, and C. Ciccotelli, "B-CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics", *OASIcs, Volume 71, Tokenomics 2019*, vol. 71, p. 12:1-12:15, 2020.

[11] Sakshi, A. Malik, and A. K. Sharma, "A survey on blockchain based IoT forensic evidence preservation: research trends and current challenges", *Multimed Tools Appl*, vol. 83, no. 14, pp. 42413–42458, Apr. 2024.

[12] D. Batista *et al.*, "Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review", *JRFM*, vol. 16, no. 8, p. 360, Aug. 2023.

[13] 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", *TecnoL.*, vol. 27, no. 60, p. e3049, Aug. 2024.

[14] A. J. Akbarfam, M. Heidaripour, H. Maleki, G. Dorai, and G. Agrawal, "ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability", Aug. 07, 2023.

[15] H. F. Atlam, N. Ekuri, M. A. Azad, and H. S. Lallie, "Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions", *Electronics*, vol. 13, no. 17, p. 3568, Sep. 2024.

[16] T. K. Dasaklis, F. Casino, and C. Patsakis, "SoK: Blockchain Solutions for Forensics", in *Technology Development for Security Practitioners*, B. Akhgar, D. Kavallieros, and E. Sdongos, Eds., in Security Informatics and Law Enforcement. , Cham: Springer International Publishing, 2021, pp. 21–40.