Blockchain as a Tool to Improve Chain of Custody Procedures in Digital Forensics: A Systematic Review

Katherine Indira Ponte Cuevas; [1]; Arnold Anthony Huaman Aguirre[2]
[1,2]Universidad Tecnológica del Perú, Lima, Perú, *U18210051@utp.edu.pe, C19532@utp.edu.pe*

Abstract*– This review article analyses the impact of blockchain technology on the management of the chain of custody of digital evidence in forensic analysis. Fifteen relevant studies were examined to identify the specific procedures used, the improvements introduced by blockchain, the differences with traditional methods, and the metrics used to evaluate its effectiveness. The results highlight that blockchain offers significant advantages in terms of integrity, traceability, reliability, and efficiency, overcoming the limitations of traditional methods based on centralized and manual records. The most prominent procedures include the use of hashing to ensure the immutability of records, precise timestamps to guarantee traceability, and redundancy through distributed nodes to prevent data loss. Blockchain improves transparency and security, allowing real-time access and reducing human errors through automation with smart contracts. Furthermore, metrics such as consensus rate and resilience demonstrated the robustness of the system in adverse scenarios, while challenges related to energy consumption and interoperability underline the need for more sustainable solutions. It is concluded that blockchain is a transformative technology for digital forensics, capable of redefining evidence custody standards. However, it is essential to address technical and economic challenges through the establishment of global standards and interdisciplinary collaboration to maximize its potential in practical and diverse environments. This work contributes to the understanding of blockchain as a key tool to strengthen forensic processes in the management of digital evidence.

***Keywords*-- Blockchain, chain of custody, digital forensics.**

Blockchain como Herramienta para Mejorar los Procedimientos de Cadena de Custodia en el Análisis Forense Digital: Una Revisión Sistemática

Katherine Indira Ponte Cuevas; [1]; Arnold Anthony Huaman Aguirre[2]
[1,2]Universidad Tecnológica del Perú, Lima, Perú, *U18210051@utp.edu.pe, C19532@utp.edu.pe*

Resumen*– Este artículo de revisión analiza el impacto de la tecnología blockchain en la gestión de la cadena de custodia de la evidencia digital en análisis forense. Se examinaron 15 estudios relevantes para identificar los procedimientos específicos utilizados, las mejoras introducidas por blockchain, las diferencias con los métodos tradicionales y las métricas empleadas para evaluar su efectividad. Los resultados destacan que blockchain ofrece ventajas significativas en términos de integridad, trazabilidad, confiabilidad y eficiencia, superando las limitaciones de los métodos tradicionales basados en registros centralizados y manuales. Los procedimientos más destacados incluyen el uso de hashing para asegurar la inmutabilidad de los registros, marcas de tiempo precisas para garantizar la trazabilidad y redundancia mediante nodos distribuidos para evitar la pérdida de datos. Blockchain mejora la transparencia y la seguridad, permitiendo acceso en tiempo real y reduciendo errores humanos mediante automatización con contratos inteligentes. Además, las métricas como la tasa de consenso y la resiliencia demostraron la robustez del sistema en escenarios adversos, mientras que los desafíos relacionados con el consumo energético y la interoperabilidad subrayan la necesidad de soluciones más sostenibles. Se concluye que blockchain es una tecnología transformadora para el análisis forense digital, capaz de redefinir los estándares de custodia de evidencia. No obstante, es esencial abordar los desafíos técnicos y económicos mediante el establecimiento de estándares globales y la colaboración interdisciplinaria para maximizar su potencial en entornos prácticos y diversos. Este trabajo contribuye al entendimiento de blockchain como herramienta clave para fortalecer los procesos forenses en el manejo de evidencia digital.

Palabras clave—Blockchain, cadena de custodia, análisis forense digital.

I. Introducción

En los últimos años, el análisis forense digital ha ganado una relevancia significativa en el ámbito empresarial debido al aumento en la frecuencia y complejidad de fraudes corporativos y financieros. La informática forense digital proporciona herramientas y metodologías esenciales para investigar irregularidades en los sistemas informáticos, permitiendo detectar y prevenir actividades fraudulentas de manera precisa y eficiente [1], [2]. Dentro de este campo, la gestión de la evidencia digital bajo procedimientos robustos de cadena de custodia se ha identificado como un factor crítico para garantizar la validez legal y la integridad de la evidencia recopilada.

La cadena de custodia, entendida como el conjunto de procedimientos que documentan la recolección, transferencia, análisis y almacenamiento de evidencia, es fundamental para preservar su integridad durante un proceso de investigación forense. Sin embargo, una revisión de la literatura revela desafíos persistentes en su implementación, como la falta de estándares universales, el uso limitado de tecnologías avanzadas y deficiencias en la capacitación del personal encargado de gestionar la evidencia [3], [4], [5]. Estas limitaciones pueden comprometer la validez de la evidencia digital en entornos judiciales, dificultando la resolución de incidentes de seguridad y de casos de fraude.

En este contexto, el blockchain ha emergido como una tecnología prometedora para abordar los desafíos asociados a la cadena de custodia en el análisis forense digital [6], [7], [8]. Sus características inherentes, como la inmutabilidad, la trazabilidad y la transparencia, la convierten en una herramienta potencialmente revolucionaria para garantizar la integridad y confiabilidad de la evidencia digital durante todo su ciclo de vida. Aunque algunos sectores han comenzado a implementar blockchain en este ámbito, su uso aún no es uniforme, y su adopción enfrenta barreras significativas en términos de costos, infraestructura y conocimiento técnico.

Este artículo presenta una revisión sistemática de la literatura enfocada en el uso de blockchain para la mejora de los procedimientos de cadena de custodia en el análisis forense digital. Se analizarán las aplicaciones actuales, los beneficios y limitaciones de esta tecnología, y su impacto en la trazabilidad y seguridad de la evidencia digital. Asimismo, se identificarán las brechas existentes en la implementación de blockchain y se explorarán las oportunidades de investigación futura para optimizar su integración en diferentes contextos forenses.

II. Metodología

A. Formulación de las preguntas de Investigación

Para garantizar la precisión y la rigurosidad del proceso de revisión, se emplearon las directrices PICOC (Population, Intervention, Comparison, Outcome, Context) [9]. Luego de identificar los elementos requeridos para alcanzar los objetivos de la revisión se plantearon las preguntas detalladas en la tabla I.

TABLA I
PREGUNTAS DE INVESTIGACIÓN PLANTEADAS A PARTIR DE LOS ELEMENTOS PICO

Elemento	Descripción	Pregunta
P	Procedimientos de análisis forense digital	¿Cuáles son los procedimientos actuales utilizados en el análisis forense digital para manejar la cadena de custodia de evidencia?
I	Implementación de la tecnología BlockChain	¿Cómo contribuye una tecnología emergente como el blockchain para mejorar los procedimientos de cadena de custodia en el análisis forense digital?
C	Diferencias con los procedimientos tradicionales	¿Qué diferencias existen entre los métodos tradicionales de gestión de cadena de custodia y aquellos que integran blockchain?
O	Impacto en la trazabilidad y confiabilidad de los datos	¿Qué métricas se utilizaron para medir la integridad, trazabilidad y confiabilidad de la evidencia digital en análisis forense?
Pregunta General:		**¿Cómo influye la implementación de blockchain en la mejora de los procedimientos de cadena de custodia en el análisis forense digital, específicamente en términos de integridad y trazabilidad de la evidencia?**

TABLA II
TÉRMINOS DE BÚSQUEDA DEL MARCO PICOC

Factor	Description	Synonymy
Problem	Digital forensic analysis procedures	*Digital Forensic Procedures, Evidence Handling, Forensic Data Management, Chain of Custody Protocols.*
Intervention	Implementation of BlockChain technology	*Blockchain Implementation, Evidence Traceability, Data Integrity, Blockchain for Chain of Custody.*
Comparison	Differences with traditional procedures	*Traditional Evidence Management, Legacy Chain of Custody Methods, Non-blockchain Solutions, Forensic Evidence Control.*
Objetive	Impact on data traceability and reliability	*Evidence Integrity, Data Traceability, Digital Evidence Reliability, Blockchain-based Evidence Security.*

B. *Estrategia de búsqueda*

Se definieron los términos específicos de búsqueda identificando las palabras clave para cada elemento, los cuales se encuentran resumidos en Tabla II. Para encontrar los artículos relevantes, se acudió a la base de datos académica de Scopus. Se tomaron las palabras clave más adecuadas y se utilizó la siguiente ecuación que fue utilizada en su motor de búsqueda:

TITLE-ABS-KEY ("Digital forensic procedures" OR "chain off custody" OR "custodial protocols") AND TITLE-ABS-KEY ("blocking" OR "evidence integrity") AND TITLE-ABS-KEY ("traceability" OR "reliability")

C. *Proceso de Selección PRISMA*

El proceso de selección de estudios siguió las directrices PRISMA[10] y se documentó en el diagrama de flujo PRISMA de la Figura 1. En primer lugar, se obtuvieron 40 estudios mediante la búsqueda en SCOPUS, excluyéndose 7 registros por tratarse de artículos de revisión previos. Se excluyeron también 3 artículos que estaban escritos en idiomas distintos al inglés. Además, no se consideraron 11 estudios debido a que no se pudo recuperar el texto completo. Los registros recuperados se evaluaron detalladamente para confirmar su elegibilidad. Los criterios de inclusión y exclusión para seleccionar los estudios se detallan a continuación.

1) Criterios de inclusión: Los criterios de inclusión fueron definidos para centrar toda la información relacionada con nuestra pregunta de investigación. Incluimos estudios

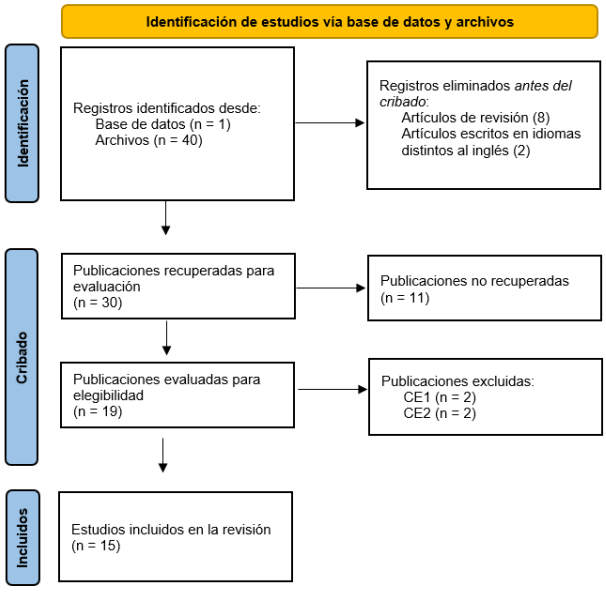

Fig. 1 Diagrama de flujo PRISMA indicando el proceso de selección de artículos.

TABLA III
CRITERIOS DE INCLUSIÓN

Código	Description
I1	Estudios que aborden procedimientos de análisis forense digital con foco en la cadena de custodia.
I2	Investigaciones que evalúen la implementación de tecnologías avanzadas como blockchain en la cadena de custodia.
I3	Artículos que comparen los métodos tradicionales de cadena de custodia con soluciones basadas en blockchain.
I4	Estudios que presenten métricas y resultados sobre integridad, trazabilidad y confiabilidad de la evidencia digital.

2) Criterios de exclusión: Los criterios de exclusión nos ayudaron a descartar información no relevante. Excluimos estudios.

TABLA IV. CRITERIO DE EXCLUSIÓN

Código	Description
E1	Estudios centrados en otras tecnologías que no incluyan blockchain (e.g., criptografía, IA sin relación directa).
E2	Trabajos que se enfoquen en áreas no relacionadas como medicina forense, recursos humanos, o educación.

Finalmente, 15 estudios cumplieron con todos los criterios de inclusión y fueron seleccionados para su inclusión en la revisión sistemática. Estos estudios proporcionaron datos y análisis relevantes que contribuyen a la evaluación y mejora de los procedimientos de cadena de custodia en el análisis forense digital, con un enfoque en la integridad y confiabilidad de los datos.

III. RESULTADOS

A. ¿Cuáles son los procedimientos actuales utilizados en el análisis forense digital para manejar la cadena de custodia de evidencia?

Los artículos revisados describieron diversas implementaciones y procedimientos innovadores que abordan la gestión de la cadena de custodia en el análisis forense digital. Los hallazgos principales se resumen en la Tabla V.

La trazabilidad fue un aspecto destacado en todos los sistemas revisados, encontrándose procedimientos que documentaban cada acceso y transferencia de la evidencia, asegurando un historial verificable [11-15]. Se identificaron, además, procedimientos de gestión automatizada con Contratos Inteligentes como B-CoC (Blockchain-Based Chain of Custody), para gestionar automáticamente la transferencia de custodia, con validaciones en tiempo real [11]. Otro estudio reportó el uso de Contratos Inteligentes en plataformas como Ethereum y Quorum para automatizar la validación y registro de transacciones relacionadas con la evidencia, reduciendo errores humanos y mejorando la eficiencia del proceso [12]. Los Contratos Inteligentes también fueron utilizados en combinación con blockchain en la trazabilidad de alimentos para optimizar la gestión en cadenas de suministro complejas [13].

TABLA V
PROCEDIMIENTOS ESPECÍFICOS UTILIZADOS PARA EL ANÁLISIS FORENSE DIGITAL

Implementación/Procedimiento	Referencia
Auditorías Automáticas y Monitoreo en Tiempo Real	[14], [15], [16], [17], [18]
Gestión Automatizada con Contratos Inteligentes	[11], [12], [13],
Sistemas basados en Hashing y Registro de Transacciones	[19], [20], [21], [22]
Uso de Almacenamiento Descentralizado	[22], [23], [24]
Validación de Acceso y Seguridad Avanzada	[24], [25]

La creación de identificadores únicos para cada evidencia mediante funciones hash (como SHA-256) fue uno de los procedimientos centrales para garantizar la integridad de los datos registrados [19-21]. Destaca la arquitectura MF-Ledger, que Integró blockchain con cifrado avanzado y almacenamiento distribuido para maximizar la seguridad y disponibilidad [22].

La descentralización mediante almacenamiento en múltiples nodos también fue una estrategia recurrente para garantizar la redundancia y disponibilidad de los datos. Esto se implementó mediante tecnologías como Filecoin y sistemas híbridos de blockchain y almacenamiento externo [22-24]. Algunos sistemas utilizaron enfoques como el cifrado basado en atributos (CP-ABE) y firmas BLS para controlar el acceso a la evidencia digital y asegurar su confidencialidad [24, 25].

Estos procedimientos reflejan la evolución hacia sistemas más seguros, eficientes y confiables en la gestión de cadenas de custodia, destacando la versatilidad y robustez de blockchain como tecnología base. Las implementaciones revisadas demuestran cómo estas soluciones pueden adaptarse a diversos contextos forenses, mejorando la integridad y trazabilidad de la evidencia digital.

B. ¿Cómo contribuye una tecnología emergente como el blockchain para mejorar los procedimientos de cadena de custodia en el análisis forense digital?

Los resultados relacionados con las mejoras introducidas por blockchain en la gestión de la cadena de custodia, se resumen en la Tabla VI. Blockchain permite a los actores autorizados acceder a los registros en tiempo real, lo que mejora la visibilidad y facilita auditorías instantáneas. Cada interacción con la evidencia queda registrada de manera transparente y accesible para las partes interesadas, asegurando confianza y claridad en los procesos [15], [13], [24]. Blockchain también garantiza que los registros sean inalterables después de su creación, eliminando la posibilidad de manipulación de la evidencia digital. Cada interacción o transacción queda documentada con detalles como el usuario, la acción realizada y una marca de tiempo. Esto asegura que cualquier alteración

sea detectable, proporcionando un historial completo y verificable de la cadena de custodia [19], [20-23].

TABLA VI
MEJORAS ESPECÍFICAS INTRODUCIDAS POR BLOCKCHAIN PARA EL ANÁLISIS FORENSE DIGITAL

Mejora	Descripción	Referencia
Transparencia en Tiempo Real	Acceso inmediato y verificable a registros por actores autorizados.	[15], [13], [24]
Inmutabilidad y Trazabilidad	Garantía de registros inalterables y rastreo completo de la evidencia.	[19], [20], [21], [22], [23]
Descentralización	Reducción de dependencia en un punto central, garantizando resiliencia.	[18], [22], [23], [24]
Reducción de Costos y Optimización	Uso de almacenamiento externo para minimizar costos en blockchain.	[18], [13]

La estructura descentralizada de blockchain elimina la dependencia de un único punto de control, reduciendo la vulnerabilidad a manipulaciones internas o ataques externos. Al distribuir los datos entre múltiples nodos, se aumenta la resiliencia del sistema y se evita que un fallo en un nodo afecte a toda la red [22-24]. Este enfoque es especialmente útil en sistemas de custodia que manejan datos críticos o grandes volúmenes de evidencia [18], [23].

Se debe mencionar tambien la ventaja que tiene algunos sistemas cuando combinan blockchain con almacenamiento externo, registrando solo los datos esenciales (como hashes o metadatos) en la blockchain y almacenando los archivos completos en servidores externos. Esto reduce los costos operativos y asegura un equilibrio entre eficiencia y escalabilidad [18], [13].

C. ¿Qué diferencias existen entre los métodos tradicionales de gestión de cadena de custodia y aquellos que integran blockchain?

Para mostrar las diferencias más importantes entre los métodos tradicionales y los sistemas basados en blockchain, se elaboró la Tabla VII. Los resultados de la revisión muestran diferencias significativas entre los métodos tradicionales de gestión de la cadena de custodia y los sistemas basados en blockchain, destacando cómo esta última tecnología aborda las limitaciones previas. En términos de confiabilidad, blockchain garantiza registros inmutables protegidos por criptografía, eliminando la vulnerabilidad a manipulaciones y errores humanos presentes en los métodos tradicionales [19], [21]. La capacidad de rastrear cada interacción con la evidencia digital de forma verificable refuerza la confianza en los procesos de custodia.

En cuanto a escalabilidad y accesibilidad, blockchain supera ampliamente las limitaciones de los métodos tradicionales, que dependen de infraestructuras centralizadas y procesos manuales. La arquitectura descentralizada de blockchain permite manejar grandes volúmenes de datos y usuarios simultáneamente, manteniendo un rendimiento óptimo [18]. Además, el acceso descentralizado y en tiempo real elimina la necesidad de intermediarios, agilizando las auditorías y mejorando la colaboración entre las partes interesadas [15].

Finalmente, blockchain destaca en eficiencia operativa, resiliencia y seguridad y privacidad. La automatización mediante contratos inteligentes reduce errores y acelera procesos como la transferencia de custodia y las auditorías [12], [24]. Su diseño distribuido asegura la continuidad de los registros incluso en caso de fallos en nodos específicos [22], mientras que la implementación de tecnologías avanzadas como el cifrado basado en atributos y las pruebas de conocimiento cero garantiza un control granular del acceso a la evidencia [23]. En conjunto, estas diferencias posicionan a blockchain como una solución robusta y confiable para la gestión de la cadena de custodia en análisis forense digital.

TABLA VII
TABLA COMPARATIVA DE LOS ASPECTOS MÁS IMPORTANTES ENTRE MÉTODOS TRADICIONALES Y BLOCKCHAIN

Aspecto	Métodos tradicionales	Sistemas basados en Blockchain
Confiabilidad	Vulnerable a errores humanos y manipulación.	Registros inmutables protegidos por criptografía.
Escalabilidad	Limitada por procesos manuales y centralizados.	Alta capacidad para manejar grandes volúmenes de datos.
Accesibilidad	Requiere intermediarios y procesos lentos.	Acceso en tiempo real y descentralizado.
Eficiencia Operativa	Dependencia de supervisión manual.	Automatización mediante contratos inteligentes.
Resiliencia	Susceptible a fallos en sistemas centralizados.	Distribución en nodos múltiples garantiza disponibilidad.
Seguridad y Privacidad	Protección básica mediante contraseñas o auditorías manuales.	Cifrado avanzado y control granular del acceso.

D. ¿Qué métricas se utilizaron para medir la integridad, trazabilidad y confiabilidad de la evidencia digital en análisis forense?

Los valores observados en las métricas utilizadas en los 15 artículos proporcionan una visión clara de la efectividad de los sistemas basados en blockchain para la gestión de la evidencia digital. La Tabla VIII presenta los resultados resumidos.

Los resultados obtenidos muestran que las métricas utilizadas en los sistemas basados en blockchain garantizan altos estándares de integridad para la evidencia digital. La generación de valores hash únicos mediante algoritmos como SHA-256 y MD5 alcanzó una tasa del 100% en detección de alteraciones, asegurando que cualquier modificación en la evidencia sea identificable de inmediato [21], [24], [26]. Además, las pruebas de inmutabilidad realizadas en simulaciones demostraron que los sistemas podían resistir completamente los intentos de manipulación, destacando la robustez de blockchain frente a ataques internos o externos [24], [25].

En términos de trazabilidad, las marcas de tiempo precisas asociadas a cada interacción con la evidencia permiten reconstruir su historial completo con exactitud, con tiempos de recuperación de registros entre 1 y 5 segundos incluso en sistemas que manejan hasta 50,000 transacciones [12], [14], [15]. Esto asegura no solo la transparencia de los procesos, sino también la eficiencia operativa, especialmente en escenarios de auditoría. La trazabilidad también se fortaleció gracias al consenso logrado por más del 95% de los nodos en redes blockchain basadas en algoritmos PoW y PoS, lo que valida la autenticidad de los registros [11], [22].

Las métricas de confiabilidad destacaron la resiliencia de los sistemas basados en blockchain. Las pruebas realizadas mostraron una disponibilidad promedio del 99.9% para los registros, incluso cuando hasta un 30% de los nodos fallaron simultáneamente [13], [23]. Esto subraya la capacidad de los sistemas para mantener la evidencia accesible y confiable en escenarios críticos. En conjunto, estas métricas validan la implementación de blockchain como una tecnología clave para optimizar la gestión de la cadena de custodia en análisis forense digital, superando significativamente las limitaciones de los métodos tradicionales.

TABLA VIII
RESULTADOS DE LAS MÉTRICAS PARA EVALUAR LA INTEGRIDAD, TRAZABILIDAD Y CONFIABILIDAD DE LA EVIDENCIA DIGITAL EN ANÁLISIS FORENSE

Métrica	Descripción	Valores obtenidos
Hashing (SHA-256, MD5)	Generación de valores únicos por evidencia.	Tasa de detección de alteraciones: 100%.
Pruebas de Inmutabilidad	Resistencia a manipulación de registros.	Protección completa en simulaciones de ataque.
Marcas de Tiempo	Registro de interacciones con evidencia.	Precisión en milisegundos; 100% de transacciones registradas.
Cantidad de Transacciones	Total de transacciones almacenadas.	Entre 10,000 y 50,000 por sistema en escenarios de prueba.
Tiempo de Recuperación	Velocidad para recuperar historial.	Entre 1 y 5 segundos por consulta.
Tasa de Consenso	Porcentaje de nodos que validan transacciones.	Más del 95% en blockchains basadas en PoW y PoS.
Disponibilidad del Sistema	Capacidad de mantener registros accesibles.	Disponibilidad promedio del 99.9%.
Resiliencia a Fallos	Recuperación tras fallos en nodos.	Recuperación completa con fallos hasta en el 30% de los nodos.

IV. DISCUSIÓN

La revisión de los 15 artículos reveló avances significativos en la implementación de blockchain para mejorar la gestión de la cadena de custodia en análisis forense digital. Los resultados obtenidos de las cuatro preguntas permiten evaluar cómo esta tecnología aborda las limitaciones tradicionales y establece las métricas de rendimiento en términos de integridad, trazabilidad, confiabilidad y eficiencia. Sin embargo, es importante contextualizar estos hallazgos dentro de los desafíos actuales y las oportunidades futuras.

En relación con los procedimientos específicos utilizados, blockchain emerge como un estándar para la trazabilidad y la inmutabilidad de registros, con soluciones como B-CoC y MF-Ledger destacando por su capacidad para registrar cada interacción de manera inalterable [11], [22]. La integración de tecnologías complementarias como contratos inteligentes y cifrado avanzado ha permitido una gestión más precisa y segura de la evidencia digital [12], [24]. Sin embargo, estas implementaciones requieren un equilibrio entre la complejidad técnica y la usabilidad, ya que sistemas altamente sofisticados pueden presentar barreras de adopción en entornos con recursos limitados [27].

Respecto a las mejoras específicas introducidas por blockchain, los resultados confirman que esta tecnología fortalece la transparencia, reduce los riesgos de manipulación y mejora la resiliencia de los sistemas de custodia [14], [25]. Estas ventajas son particularmente críticas en escenarios forenses donde la integridad y trazabilidad de los datos determinan la validez de la evidencia en procedimientos judiciales. Sin embargo, a pesar de estas mejoras, la dependencia de nodos descentralizados plantea desafíos en términos de costos operativos y latencia en redes sobrecargadas [28]. Por lo tanto, futuras investigaciones podrían explorar soluciones híbridas que combinen blockchain con sistemas centralizados optimizados para minimizar costos y maximizar eficiencia.

Las diferencias clave entre métodos tradicionales y blockchain resaltan una transición hacia sistemas más confiables y escalables. Blockchain no solo elimina la necesidad de intermediarios, sino que también habilita accesos en tiempo real y facilita auditorías automatizadas [22], [23]. Esto contrasta con los procesos tradicionales, propensos a errores manuales y manipulaciones. Sin embargo, las barreras de entrada tecnológicas y económicas aún limitan la adopción masiva de blockchain en todos los contextos, especialmente en países en desarrollo [29].

Finalmente, las métricas empleadas para medir la integridad, trazabilidad y confiabilidad consolidan a blockchain como una tecnología robusta para el análisis forense digital. Las pruebas de inmutabilidad y consenso demostraron altos niveles de seguridad, mientras que la redundancia en los datos garantizó disponibilidad incluso en escenarios adversos [16], [24]. Sin embargo, la efectividad de estas métricas puede verse condicionada por desafíos técnicos subyacentes. Por ejemplo, el alto consumo energético asociado a algoritmos de consenso como Proof of Work [30], común en blockchains públicas, puede comprometer la sostenibilidad a largo plazo de los sistemas que priorizan la disponibilidad y el consenso. Asimismo, la falta de interoperabilidad entre plataformas limita la capacidad de lograr una trazabilidad y redundancia efectivas en redes descentralizadas interconectadas. Estas limitaciones resaltan la necesidad de abordar estos problemas para garantizar que los valores obtenidos en las métricas sean aplicables y sostenibles en entornos prácticos [31].

IV. Conclusiones

El presente artículo de revisión confirma que blockchain ha transformado significativamente la gestión de la cadena de custodia en análisis forense digital, superando las limitaciones de los métodos tradicionales. A través de su capacidad para proporcionar integridad, trazabilidad, confiabilidad y eficiencia, blockchain se posiciona como una tecnología esencial para garantizar que la evidencia digital sea gestionada con los más altos estándares de calidad y seguridad.

En términos de procedimientos, blockchain introduce un enfoque sistemático que asegura registros inmutables, automatización de tareas clave mediante contratos inteligentes y acceso en tiempo real a través de sistemas descentralizados. Estas características han demostrado ser efectivas para mantener la validez de la evidencia en entornos forenses críticos, especialmente en casos donde la precisión y la resistencia a manipulaciones son fundamentales.

Las mejoras específicas introducidas por blockchain, como la transparencia en tiempo real, la resistencia a fallos y la optimización de costos, destacan su valor agregado frente a los métodos tradicionales. Sin embargo, persisten desafíos técnicos y económicos, como el alto consumo energético en blockchains públicas y la necesidad de desarrollar soluciones híbridas que equilibren complejidad técnica con usabilidad y accesibilidad.

Finalmente, las métricas empleadas para evaluar la efectividad de blockchain, como hashing, marcas de tiempo, tasa de consenso y resiliencia, confirman su robustez en la gestión de la cadena de custodia. Sin embargo, desafíos como el alto consumo energético de algunos algoritmos y la falta de interoperabilidad entre plataformas limitan su aplicabilidad. Abordar estos aspectos mediante estándares globales y colaboración interdisciplinaria será crucial para maximizar su impacto en el análisis forense digital.

Referencias

[1] S. Hina and P. D. D. Dominic, "Information security policies' compliance: a perspective for higher education institutions," *Journal of Computer Information Systems*, vol. 60, no. 3, pp. 201–211, May 2020, doi: 10.1080/08874417.2018.1432996.

[2] Rosita Eberechukwu Daraojimba, Oluwatoyin Ajoke Farayola, Funmilola Olatundun Olatoye, Noluthando Mhlongo, and Timothy Tolulope Oke, "FORENSIC ACCOUNTING IN THE DIGITAL AGE: A U.S. PERSPECTIVE: SCRUTINIZING METHODS AND CHALLENGES IN DIGITAL FINANCIAL FRAUD PREVENTION," *Finance & Accounting Research Journal*, vol. 5, no. 11, pp. 342–360, Nov. 2023, doi: 10.51594/farj.v5i11.614.

[3] N. Chowdhury, S. Katsikas, and V. Gkioulos, "Modeling effective cybersecurity training frameworks: A delphi method-based study," *Comput Secur*, vol. 113, p. 102551, Feb. 2022, doi: 10.1016/j.cose.2021.102551.

[4] P. Garg, B. Gupta, A. K. Chauhan, U. Sivarajah, S. Gupta, and S. Modgil, "Measuring the perceived benefits of implementing blockchain technology in the banking sector," *Technol Forecast Soc Change*, vol. 163, p. 120407, Feb. 2021, doi: 10.1016/j.techfore.2020.120407.

[5] K. Hughes-Lartey, M. Li, F. E. Botchey, and Z. Qin, "Human factor, a critical weak point in the information security of an organization's Internet of things," *Heliyon*, vol. 7, no. 3, Mar. 2021, doi: 10.1016/j.heliyon.2021.e06522.

[6] Sakshi, A. Malik, and A. K. Sharma, "Blockchain-based digital chain of custody multimedia evidence preservation framework for internet-of-things," *Journal of Information Security and Applications*, vol. 77, p. 103579, Sep. 2023, doi: 10.1016/j.jisa.2023.103579.

[7] R. Sathyaprakasan, P. Govindan, S. Alvi, L. Sadath, S. Philip, and N. Singh, "An Implementation of Blockchain Technology in Forensic Evidence Management," in *2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, IEEE, Mar. 2021, pp. 208–212. doi: 10.1109/ICCIKE51210.2021.9410791.

[8] C.-J. Chew, W.-B. Lee, T.-H. Chen, I.-C. Lin, and J.-S. Lee, "Log Preservation in Custody Dual Blockchain With Energy Regime and Obfuscation Shuffle," *IEEE Trans Netw Sci Eng*, vol. 11, no. 4, pp. 3495–3511, Jul. 2024, doi: 10.1109/TNSE.2024.3375921.

[9] T. F. Frandsen, M. F. Bruun Nielsen, C. L. Lindhardt, and M. B. Eriksen, "Using the full PICO model as a search tool for systematic reviews resulted in lower recall for some PICO elements," *J Clin Epidemiol*, vol. 127, pp. 69–75, Nov. 2020, doi: 10.1016/j.jclinepi.2020.07.005.

[10] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *International Journal of Surgery*, vol. 8, no. 5, pp. 336–341, 2010, doi: 10.1016/j.ijsu.2010.02.007.

[11] S. Bonomi, M. Casini, and C. Ciccotelli, "B-CoC: A blockchain-based chain of custody for evidences management in digital forensics," in *OpenAccess Series in Informatics*, Schloss Dagstuhl- Leibniz-Zentrum fur Informatik GmbH, Dagstuhl Publishing, Mar. 2020. doi: 10.4230/OASIcs.Tokenomics.2019.12.

[12] 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, Apr. 2023, doi: 10.3390/smartcities6020034.

[13] P. Azevedo, J. Gomes, and M. Romão, "Supply chain traceability using blockchain," *Operations Management Research*, vol. 16, no. 3, pp. 1359–1381, Sep. 2023, doi: 10.1007/s12063-023-00359-y.

[14] S. L. Bager, C. Singh, and U. M. Persson, "Blockchain is not a silver bullet for agro-food supply chain sustainability: Insights from a coffee case study," *Current Research in Environmental Sustainability*, vol. 4, Jan. 2022, doi: 10.1016/j.crsust.2022.100163.

[15] F. Yun-Yi, C. Chit-Jie, H. Wei-Che, C. Ying-Chin, and L. Jung-San, "Blockchain-based Pipeline Custody System (BPCS) for Preserving Critical Video Evidence," *Journal of Internet Technology*, vol. 25, no. 3, pp. 447–454, 2024, doi: 10.53106/160792642024052503010.

[16] A. Shehata, H. K. Aslan, Y. I. Cho, and M. S. Abdallah, "Micro Cloud Services Forensics as a Framework," *International Journal of Safety and Security Engineering*, vol. 14, no. 2, pp. 421–433, Apr. 2024, doi: 10.18280/ijsse.140210.

[17] F. C. Tsai, "The application of blockchain of custody in criminal investigation process," in *Procedia Computer Science*, Elsevier B.V., 2021, pp. 2779–2788. doi: 10.1016/j.procs.2021.09.048.

[18] L. E. Cartier, S. H. Ali, and M. S. Krzemnicki, "Blockchain, chain of custody and trace elements: An overview of tracking and traceability opportunities in the gem industry," *Journal of Gemmology*, vol. 36, no. 3, pp. 212–227, 2018, doi: 10.15506/JoG.2018.36.3.212.

[19] F. Calvão and M. Archer, "Digital extraction: Blockchain traceability in mineral supply chains," *Polit Geogr*, vol. 87, May 2021, doi: 10.1016/j.polgeo.2021.102381.

[20] G. Mugurusi and E. Ahishakiye, "Blockchain technology needs for sustainable mineral supply chains: A framework for responsible sourcing of Cobalt.," in *Procedia Computer Science*, Elsevier B.V., 2022, pp. 638–647. doi: 10.1016/j.procs.2022.01.262.

[21] O. Olukoya, "Distilling blockchain requirements for digital investigation platforms," *Journal of Information Security and Applications*, vol. 62, Nov. 2021, doi: 10.1016/j.jisa.2021.102969.

[22] 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, 2021, doi: 10.1109/ACCESS.2021.3099037.

[23] W. Silva and A. C. B. Garcia, "Where is our data? A Blockchain-based Information Chain of Custody Model for Privacy Improvement," in

Proceedings of the 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2021, Institute of Electrical and Electronics Engineers Inc., May 2021, pp. 329–334. doi: 10.1109/CSCWD49262.2021.9437727.

[24] W. Yan, J. Shen, Z. Cao, and X. Dong, "Blockchain Based Digital Evidence Chain of Custody," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Mar. 2020, pp. 19–23. doi: 10.1145/3390566.3391690.

[25] A. O. Charles, A. Oguntimilehin, and O. A. Bello, "Forensic Evidence Security System using Blockchain Technology," *International Journal of Engineering Trends and Technology*, vol. 71, no. 8, pp. 143–151, Aug. 2023, doi: 10.14445/22315381/IJETT-V71I8P212.

[26] F. Calvão and M. Archer, "Digital extraction: Blockchain traceability in mineral supply chains," *Polit Geogr*, vol. 87, p. 102381, May 2021, doi: 10.1016/j.polgeo.2021.102381.

[27] O. Ozbal, T. Duman, and O. Topaloglu, "A trust-based peer-to-peer digital brand equity (P2P-DBE) model," *Journal of Marketing Theory and Practice*, vol. 28, no. 4, pp. 497–520, Oct. 2020, doi: 10.1080/10696679.2020.1794901.

[28] H. Fan, Y. Liu, and Z. Zeng, "Decentralized Privacy-Preserving Data Aggregation Scheme for Smart Grid Based on Blockchain," *Sensors*, vol. 20, no. 18, p. 5282, Sep. 2020, doi: 10.3390/s20185282.

[29] D. di Prisco and D. Strangio, "Technology and financial inclusion: a case study to evaluate potential and limitations of Blockchain in emerging countries," *Technol Anal Strateg Manag*, pp. 1–14, Jun. 2021, doi: 10.1080/09537325.2021.1944617.

[30] N. Lasla, L. Al-Sahan, M. Abdallah, and M. Younis, "Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm," *Computer Networks*, vol. 214, p. 109118, Sep. 2022, doi: 10.1016/j.comnet.2022.109118.

[31] A. Miglani, N. Kumar, V. Chamola, and S. Zeadally, "Blockchain for Internet of Energy management: Review, solutions, and challenges," *Comput Commun*, vol. 151, pp. 395–418, Feb. 2020, doi: 10.1016/j.comcom.2020.01.014.