

**BLOCKCHAIN EN MEDICINA LEGAL Y FORENSE: APLICACIONES, DESAFÍOS E INFLUENCIA****BLOCKCHAIN IN FORENSIC AND LEGAL MEDICINE: APPLICATIONS, CHALLENGES, AND INFLUENCE**

Romero García LD.  
Odontólogo  
Valencia.  
España.

Correspondencia: forense Luisda@gmail.com

**Resumen:** Actualmente, la tecnología blockchain es una revolución como un recurso muy positivo para aumentar la seguridad, la inmutabilidad, la trazabilidad y la transparencia en la gestión de datos digitales. En el área de la medicina forense y legal no ha sido la excepción en donde la integridad de los datos, la cadena de custodia y la gestión de evidencias son elementos fundamentales y que con esta tecnología brinda nuevos enfoques de uso.

Este artículo presenta una revisión narrativa de la literatura científica disponible a partir del 2017, sobre el empleo de la tecnología blockchain en escenarios médico-legales y forenses y su ejecución en situaciones reales, explorando sus aplicaciones y desafíos.

Los resultados de esta revisión han mostrado que desde su origen de esta tecnología ha habido interés en aplicarla a contextos forenses, desde el registro inmutable de las evidencias así como de la cadena de custodia digital y la protección de los registros clínicos-jurídicos para potenciar la interoperabilidad entre sistemas de justicia y de salud, reconociendo sus posibilidades de uso y los retos existentes en el área ética (privacidad de datos sensibles); técnica (escalabilidad, consumo energético) y jurídica (cumplimiento normativo) que condicionan su ejecución. Un caso práctico en Pakistán (NGO-RMSD) ilustra la viabilidad de blockchain en entornos críticos.

Finalmente, se sugiere promover investigaciones con aplicación de modelos usando esta tecnología para facilitar la adopción ética y efectiva con la realización de proyectos piloto para confirmar su eficacia en contextos reales en diferentes escenarios. No obstante, con las limitaciones de esta revisión narrativa, se pretende contribuir al entendimiento interdisciplinario de la tecnología blockchain en Medicina Legal, impulsando posibles vías de investigación.

**Palabras clave:** blockchain, medicina legal, ciencias forenses, cadena de custodia, evidencia digital, tecnología.

**Abstract:** Currently, blockchain technology is revolutionizing as a very positive resource for increasing security, immutability, traceability, and transparency in digital data management. This has been no exception in the areas of forensic and legal medicine, where data integrity, chain of custody, and evidence management are fundamental elements, and this technology offers new approaches to its use.

This article presents a narrative review of the scientific literature available since 2017 on the use of blockchain technology in forensic and medical settings and its implementation in real-life situations, exploring its applications and challenges.

The results of this review have shown that since its inception, there has been interest in applying this technology to forensic contexts, from the immutable recording of evidence as well as the digital chain of custody and protecting clinical-legal records to enhance interoperability between justice and healthcare systems. Recognizing its potential uses and the existing challenges in the ethical area (privacy of sensitive data). Technical (scalability, energy consumption) and legal (regulatory compliance) factors that determine its implementation. A practical case study in Pakistan (NGO-RMSD) illustrates the viability of blockchain in critical environments.

Finally, we suggest promoting research with the application of models using this technology to facilitate ethical and effective adoption by conducting pilot projects to confirm its effectiveness in real-life contexts across different settings. Despite the limitations of this narrative review, we aim to contribute to an interdisciplinary understanding of blockchain technology in Forensic Medicine, promoting potential avenues for research.

**Keywords:** blockchain, forensic medicine, forensic sciences, chain of custody, digital evidence, technology.

## 1. INTRODUCCIÓN

La medicina legal y forense juega un papel crucial en la implementación de las leyes, aportando lo conocimientos médicos y biológicos como evidencias científicas que respaldan las resoluciones jurídicas en los casos civiles, penales y administrativos [1]. La confiabilidad de estas evidencias se basa en tres pilares clave: la integridad de

los datos, la trazabilidad de la cadena de custodia y la transparencia en los procedimientos forenses [2]. Sin embargo, se considera que uno de los principales problemas es la pérdida de datos, causada por la gestión manual de registros y la falta de sistemas unificados, así como de la manipulación y la falta de interoperabilidad entre instituciones jurídicas y de salud. [3,4]. Como sucedió en el caso de O.J. Simpson, donde la mala gestión de la escena del crimen y las equivocaciones en la documentación de las evidencias generaron inquietudes acerca de su confiabilidad, debilitando así el caso. Por otro lado, subraya la importancia de protocolos más rigurosos y más eficiencias en los sistemas de registro [5].

En 2008, Satoshi Nakamoto introduce la blockchain como base de Bitcoin [6], una tecnología, que sin ninguna duda, ha progresado más allá de las criptomonedas. Blockchain es un libro mayor distribuido, que a través de criptografía sofisticada, guarda información de cualquier tipo, registra transacciones de manera inmutable, descentralizada y transparente [7]. Esta tecnología, en el sector sanitario, ha demostrado su habilidad para proteger las historias clínicas de los pacientes, además de asegurar la trazabilidad de medicamentos y fomentar la interoperabilidad entre diferentes sistemas [8,9]. Por ejemplo, en Estonia, se está utilizando el sistema E-Residency para garantizar la protección de los datos médicos con tecnología blockchain [10], mientras que en Singapur respalda el uso de blockchain en los registros jurídicos bajo la Ley de Transacciones Electrónicas (ETA) [11]. Estas aplicaciones proponen un posible cambio en la medicina legal y forense, donde la seguridad y la trazabilidad son fundamentales.

Asimismo, en el campo forense, la tecnología blockchain puede enfrentar retos como la manipulación de evidencias, la falta de normalización en la cadena de custodia y la protección de información delicada [12]. Este artículo es una revisión narrativa de la bibliografía científica disponible (2017-2025) sobre las aplicaciones de blockchain en medicina legal y forense en la gestión de evidencias, la cadena de custodia y la seguridad de datos. Se analizan las ventajas, los retos técnicos, jurídicos y éticos, así como el posible efecto en los procesos con un caso práctico que demuestra su uso en contextos reales. Finalmente, se sugieren recomendaciones para la implementación de blockchain en entidades forenses y su incorporación a tecnologías en desarrollo.

## 2.MATERIAL Y MÉTODOS

Se realizó una revisión exhaustiva mediante la búsqueda bibliografía científica en bases de datos académicas como Scopus, PubMed, IEEE Xplore y Google Scholar y DOAJ. Los términos de búsqueda utilizados contenían abreviaturas en español e inglés de “blockchain”, “medicina legal”, “ciencias forenses”, “cadena de custodia”, “evidencia digital” y “seguridad de datos”, utilizando operadores booleanos (AND, OR, NOT) para mejorar los hallazgos. Se incluyeron artículos escritos desde el 2017. Debido a la amplitud del tema, se encontraron 512 documentos. Tras revisar títulos y resúmenes, se descartó los estudios duplicados y no relacionados con el ámbito forense, como, por ejemplo, los que se centraban en criptomonedas, solo siendo útiles 342 artículos. En esta etapa mi interés fue hacia las aplicaciones prácticas, como la gestión de evidencias o la seguridad de datos, que son fundamentales en el trabajo forense.

Se continuo con la evaluación de estos documentos para seleccionar sólo aquellos con mayor rigor y relevancia. Basándome en criterios como la calidad metodológica y la aplicabilidad de la blockchain a la medicina legal y forense, adaptando ideas de PRISMA aunque no se siguió un enfoque sistemático estricto (13). La **Tabla 1** muestra los criterios de inclusión y selección tenidos en cuenta para el desarrollo de la investigación. Siendo seleccionados finalmente para el estudio 33 artículos.

| Criterios de inclusión:   | Criterios de exclusión:   |
|---|---|
| <ul style="list-style-type: none"> <li>• Artículos académicos, revisiones, trabajos de fin de máster, tesis doctorales o informes técnicos que contemplaran aplicaciones de <u>blockchain</u> en medicina legal y forense, así como de la cadena de custodia, la gestión de evidencias o sectores relacionados.</li> <li>• Estudios que analizaran los desafíos a nivel técnico, legales o éticos de <u>blockchain</u> en contextos forenses o similares.</li> <li>• Publicaciones en revistas indexadas, conferencias relevantes o repositorios académicos.</li> </ul> | <ul style="list-style-type: none"> <li>• Artículos con falta de metodología clara o no revisado por pares</li> <li>• Trabajos que no tuvieran relación con <u>blockchain</u> o medicina legal y forense.</li> <li>• Publicaciones obsoletas o irrelevantes para los objetivos de este trabajo.</li> </ul> |

**Tabla 1.** Criterios de inclusión y exclusión

Los hallazgos se estructuran en tres fundamentos: las aplicaciones técnicas, sus ventajas y limitaciones, y la visión o perspectiva futura haciendo comparaciones, inferencias y el reconocimiento de hallazgos importantes, siempre desde la perspectiva del impacto de la tecnología blockchain, enfatizando coincidencias, diferencias y los desafíos en desarrollo de ambas áreas. Asimismo, se analizará un caso real donde se ha implementado dicha tecnología.

### 3.RESULTADOS

Esta revisión aborda algunos temas comunes y otros aspectos específicos de la aplicación, como el análisis comparativo de las aplicaciones de blockchain, resumiendo los hallazgos de la bibliográfica en el campo de Forense Digital y Medicina en la **Tabla 2**, destacando sus prioridades, tecnologías empleadas y desafíos, así como de la falta de estandarización y la escalabilidad, para evaluar su impacto y viabilidad en contextos reales.

#### 3.1 Análisis Comparativo de Aplicaciones de blockchain

En los artículos revisados respecto a el área Forense Digital (16, 20, 21,27, 28, 29, 30, 33, 34 y 35) dan prioridad a la integridad, autenticidad y trazabilidad de las evidencias, haciendo hincapié en la evidencia digital. Tal es el caso en concreto de Tsai et al. 2021 (21) donde proponen un marco en base en Ethereum para la CoC en las investigaciones criminales, mientras que Liu & Zheng (2024) integran IPFS en una base de datos descentralizado más eficiente. (29)

En los estudios de Li et al. 2021 (18) y Atlam et al. 2024 (30), exploran la blockchain forense en la detección de fraudes en criptomonedas; asimismo, en el estudio de Adere en 2022, integran la blockchain con IoT para la gestión de datos médicos, garantizando la integridad y trazabilidad de datos en tiempo real; la recolección de las evidencias digitales desde dispositivos IoT, destacando que esta integración, podrían ser viables en las ciudades inteligentes. (24)

Actualmente, Qi An et al., en 2025, han aplicado blockchain y aprendizaje profundo (YOLOv5) en la gestión de evidencia de accidentes de tráfico, con una precisión del 92.4% en la extracción automática de evidencia, confirmando la aplicabilidad práctica de blockchain combinada con técnicas de IA en el entorno forense (35), siendo también consistente en el estudio de Vaishali y Vijayakanthan porque manifiestan que puede mejorar la gestión de salud (análisis predictivo y tratamientos personalizados) y podría apoyar al contexto forense para optimizar la validación de las evidencias digitales. (37)

Por otro lado, en el campo general de la medicina, hay estudios que han focalizado a una gestión segura de los datos médicos. (14,17,19,25,26). En el estudio de Litvin et al., hacen un análisis al proyecto Medicalchain, donde destacan las aplicaciones en EHR y pruebas clínicas. (17). Por otro lado, Ortiz-Lizcano et al., hacen una

implementación práctica utilizando IBM Hyperledger Fabric en los biobancos, con ello, están asegurando la trazabilidad y confidencialidad de las muestras biológicas mediante los contratos inteligentes. Se ha diseñado un sistema donde están abordando la falta de estandarización y facilitando la interoperabilidad entre biobancos, aunque se existen fragilidad ante posibles ataques de denegación de servicio. (25) Mientras tanto, Reegu et al., mencionan la interoperabilidad de EHR mediante blockchain, proponiendo una arquitectura de tres capas que combina almacenamiento local, blockchain con Hyperledger Fabric e IPFS. Este modelo refuerza la seguridad, inmutabilidad y control de acceso, aspectos críticos en la protección de datos de salud. (26)

Manteniendo esta línea, en 2022, en el estudio de Adere se usa blockchain pública y privada junto con IoT para la gestión de los registros médicos y de los medicamentos. Con ello, han visto la mejoría de la privacidad del paciente y la trazabilidad (24) aunque se mantiene el reto de la recuperación de datos y la interoperabilidad como en otros estudios encontrados. (25,26)

En Sri Lanka, Vaishali y Vijayakanthan (2025) destacan que blockchain puede mejorar los sistemas EHR, la trazabilidad farmacéutica, los sistemas de telemedicina, la gestión de ensayos clínicos y verificación de colegiaciones médicas, encontrando desafíos similares de los presentados en los biobancos. Proponiendo modelos de almacenamiento híbrido (on-chain/off-chain) como solución y crear protocolos estandarizados como HL7 FHIR para tratar estas limitaciones (37), lo que refuerza las propuestas de Reegu et al. (26).

Ambos campos (medicina/forense) tienen como objetivo aprovechar la descentralización, inmutabilidad y seguridad de la tecnología blockchain, aunque discrepan en sus prioridades: el campo forense digital resalta la auditabilidad y la defensa legal, mientras que la medicina prioriza la privacidad del paciente (protección de datos) y la interoperabilidad.

### *3.2 Implementación Técnica*

Las implementaciones forenses varían según el tipo de blockchain y las tecnologías complementarias. En el estudio de Tsai et al., usan una blockchain privada de Ethereum con smart-contracts en Solidity para funciones como CreateEvidence y Transfer (21) mientras tanto, Liu & Zheng, hacen la combinación de Ethereum con IPFS para almacenamiento fuera de la blockchain, con ello han visto que se ha mejorado la escalabilidad.(29) Sin embargo, en los estudios del 2024, han utilizado cadenas de consorcio para aplicaciones en IoT y multimedia (29,30), aunque en el estudio de 2021 de Olukoya integraba Hyperledger Fabric con plataformas SIRP (20). Recientemente Qi An et al., hacen la combinación de blockchain de consorcio, IPFS y el modelo YOLO-MBC, donde se ha resaltado una alta precisión. (35) No obstante, previo a este estudio, Patil et al. (33) y Batista et al. (28) proponen arquitecturas como Block-DEF y B-CoC, donde están utilizando hash y codificación Base64.

En 2025, proponen como soluciones técnicas el uso de IPFS para el almacenamiento off-chain de las imágenes, combinando encriptación en blockchain para mejorar la escalabilidad. Recomiendan usar algoritmos de consenso como Proof of Stake (PoS) y Byzantine Fault Tolerance (BFT) para tener un rendimiento óptimo similares a blockchain de consorcio. (37)

En estos estudios, se observa que la elección entre cadenas privadas y de consorcio están teniendo un equilibrio entre el control y la accesibilidad. Donde IPFS está disminuyendo limitaciones de almacenamiento, aunque hay una falta de estandarización, como señala Atlam et al., lo que provoca que sea difícil la interoperabilidad. (30) En nuestros días, están proponiendo frameworks como Polkadot o Cosmos para conectar diferentes redes blockchain. (37)

Es una realidad que, en medicina, el uso de Ethereum y Hyperledger Fabric están predominando más. Desde el 2019 en el proyecto de Medicalchain se están usando contratos inteligentes para EHR (17) hasta que en el 2023 se está implementando el uso de Hyperledger Fabric para los biobancos, con contratos que tiene como objetivo gestionar el

almacenamiento y la transferencia de muestras. (25) También sugieren integrar blockchain con IoT para la recolección de evidencias en tiempo real. (37)

Sin embargo, en otros estudios, se han propuesto la elaboración de arquitecturas de 3 capas con Hyperledger, IPFS y estándares como HL7 e HIPAA (24). Se usa Hyperledger Fabric por su manejo de permisos, mientras que el usar IPFS se observa que hay mejor escalabilidad. Ahora bien, con la integración de IA, como en Doc.ai (17) se agrega un valor más analítico, pero está complicando la validación aunque se podría conseguir usando la IA en sistemas de registros médicos en combinación con la gestión de datos de investigación aunque también advierten que hay que hacer pruebas de conocimiento cero (zero-knowledge proofs) para garantizar la privacidad del paciente. (24,37) Es importante resaltar que en el estudio del 2018 de Roman-Belmonte et al., sugieren smart-contracts para consentimientos informados. (14).

**Tabla 2.** Comparativo de Aplicaciones de Blockchain en Forense Digital y Medicina

| Autor/Ref.                        | Campo           | Objetivo Principal   | Tecnologías Utilizadas                               | Beneficios Clave   | Desafíos Reportados  |
|-----------------------------------|-----------------|--|--|--|--|
| Liu, S. & Zheng, Q. (29)          | Forense Digital | Integridad de evidencias digitales                         | Ethereum + IPFS                                      | -Escalabilidad<br>-Descentralización   | Interoperabilidad limitada   |
| Atlam HF., et al. (30)            | Forense Digital | Detectar fraude en criptomonedas, IoT y multimedia forense | Blockchain de consorcio, Hash                        | -Seguridad<br>-Detección automatizada  | Existe falta de estandarización  |
| An, Q, et al. (35)                | Forense Digital | Gestión de Evidencia de accidentes con IA                  | Blockchain consorcio + IPFS + YOLOv5                 | -Precisión del 92.4%   | Complejidad técnica  |
| Patil, H., et al. (33)            | Forense Digital | Custodia de evidencias                                     | Block-DEF, codificación Base64                       | Trazabilidad, autenticidad   | Escalabilidad  |
| Olukoya, O. (20)                  | Forense Digital | Integración en plataformas de respuesta a incidentes       | Hyperledger Fabric + SIRP                            | Gestión de incidentes eficiente  | Integración compleja   |
| Suryanarayanan, H.G. (16)         | Forense Digital | Preservación digital de evidencias                         | Blockchain público                                   | Inmutabilidad, auditabilidad   | Riesgos de acceso no autorizado  |
| D'Anna, T., et al. (27)           | Forense Digital | Gestión digital de evidencia forense                       | Ethereum + contratos inteligentes                    | Registro transparente  | Validación técnica   |
| Batista, D., et al. (28)          | Forense Digital | Trazabilidad de evidencia (modelo B-CoC)                   | B-CoC, codificación Base64, Blockchain privada       | -Integridad<br>-Seguridad  | Interoperabilidad  |
| Su, Z. (34)                       | Forense Digital | Confianza en la cadena de custodia                         | Blockchain, IoT, criptografía                        | Pruebas verificables   | Falta de estandarización   |
| Tsai, F.-C. (21)                  | Forense Digital | CoC en investigaciones criminales                          | Ethereum + contratos Solidity                        | -Transparencia<br>-Validación  | -Escalabilidad<br>-Validación  |
| Litvin, A., et al. (17)           | Medicina        | Gestión de EHR y análisis clínico                          | -Medicalchain (Ethereum),<br>-Doc.ai (IA)            | -Privacidad<br>-Automatización<br>-Analítica avanzada  | -Validación de IA<br>-Interoperabilidad                                |
| Roman-Belmonte JM., et al. (14)   | Medicina        | Consentimiento informado electrónico                       | Smart-contracts                                      | -Transparencia<br>-Control de paciente   | Marco regulatorio complejo   |
| Indumathi J. (19)                 | Medicina        | Seguridad de datos médicos                                 | Blockchain pública                                   | -Inmutabilidad<br>-Descentralización   | Escalabilidad  |
| Ortiz-Lizcano, M.L., et al. (25)  | Medicina        | Trazabilidad en biobancos                                  | Hyperledger Fabric + contratos inteligentes          | -Confidencialidad<br>-Interoperabilidad entre biobancos                                      | -Riesgo de DoS (Denegación de Servicio)<br>-Falta de estandarización   |
| Reegu, F.A., et al. (26)          | Medicina        | Interoperabilidad de EHR                                   | Arquitectura 3 capas: local + Hyperledger + IPFS     | -Seguridad<br>-Escalabilidad   | -Complejidad en integración<br>-Mantenimiento                          |
| Adere EM. (24)                    | Medicina        | Gestión de datos médicos (EHR), con IoT                    | -Blockchain (pública/privada)<br>-IoT                | -Seguridad<br>-Privacidad<br>-Trazabilidad   | -Escalabilidad<br>-Interoperabilidad<br>-Estandarización               |
| Vaishali R, Vijayakanthan G. (37) | Medicina        | -Gestión segura de EHR<br>-Telemedicina                    | Hyperledger Fabric, IPFS, PoS/BET, HL7 FHIR, IoT, IA | -Privacidad<br>-Trazabilidad<br>-Interoperabilidad<br>-Automatización<br>-Seguridad de datos | -Escalabilidad,<br>-Falta de estandarización<br>-Barreras regulatorias |

### 3.3 Caso Práctico: NGO-RMSD en Pakistán

Un caso donde se usó esta herramienta fue la que desarrolló la ONG **Rural Medical Services & Development (RMSD)**, adoptando con éxito esta tecnología después del terremoto de magnitud 5.7 en Baluchistán, Pakistán, gestionando su operación humanitaria. Los autores han innovado con el uso de blockchain privada/permissioned (Quorum) para registrar de una forma distribuida, segura y transparente (cada transacción quedó registrada de forma inmutable); las necesidades, apoyos, y flujos de recursos, emplearon smart-contracts y nodos representativos de cada ONG. Se implementaron tecnologías estándar (Docker, NodeJS, Solidity). Realizaron pruebas con cinco nodos donde simularon con éxito el funcionamiento del sistema. En cuanto a las regulaciones de protección de datos (GDPR y Ley turca KVKK) no lo almacenaron en la blockchain sino que lo hicieron en bases privadas controladas por cada ONG. (22) La **Tabla 3** compara el sistema NGO-RMSD con métodos tradicionales.

**Tabla 3.** Comparativa modelo tradicional VS Sistema NGO-RMSD

| <b>Criterio</b>                   | <b>Modelos tradicionales</b>  | <b>Sistema NGO-RMSD (Blockchain)</b>   |
|-----------------------------------|---|--|
| <b>Trazabilidad</b>               | Limitada, dependiente de registros manuales/centralizados.            | Totalmente trazable, registros inmutables  |
| <b>Transparencia</b>              | Tendente a opacidad o manipulación                                    | Transparente, auditable en tiempo real   |
| <b>Seguridad (Datos)</b>          | Vulnerable a pérdida o manipulación                                   | -Alta seguridad criptográfica<br>-Integridad garantizada (25).                           |
| <b>Cadena de custodia</b>         | Difícil de verificar en entornos <u>multiexpertos</u>                 | Verificable y automatizada mediante <u>smart-contracts</u> (33).                         |
| <b>Interoperabilidad</b>          | Fragmentada, con duplicidades   | Sincronizada entre nodos ONG/forenses con reglas comunes                                 |
| <b>Gestión (Permisos y Roles)</b> | Centralizada y sujeta a errores                                       | -Descentralizada<br>-Validación por pares.   |
| <b>Protección de datos</b>        | Riesgo alto de incumplimiento normativo                               | Cumple GDPR/KVKK (Art. 25)<br>Datos sensibles fuera del <u>blockchain</u>                |
| <b>Auditoría externa</b>          | Costosa y lenta   | Inmediata, transparente y descentralizada.   |
| <b>Escalabilidad</b>              | Baja: requiere infraestructura física y reorganización institucional. | Alta: basada en nodos virtuales (Docker, Web3JS).  |
| <b>Utilidad forense</b>           | Limitada a sistemas legales/policiales.                               | Aplicable a medicina legal, identificación de víctimas, custodia y gestión de evidencia. |

El estudio de RMSD evidencia que la tecnología blockchain es efectiva y factible en situaciones críticas. Reduciendo la corrupción, potenciando la cooperación entre las instituciones, mejorando la distribución de los recursos vitales y asegurando el acceso a datos críticos durante las etapas de respuesta y recuperación. Por lo tanto, se abre nuevas perspectivas para la actualización y fortalecimiento de la práctica forense, haciendo que la tecnología blockchain sea una herramienta innovadora para que la justicia sea más transparente, segura y sobre todo, resiliente. (21) (34)

#### 4.DISCUSIÓN

La tecnología Blockchain está evolucionando a la Medicina Legal y Forense con ventajas transformadoras y abordando las limitaciones que se encuentran en los sistemas tradicionales. A diferencia de las bases de datos centralizadas, que son vulnerables a ciberataques, la inmutabilidad de esta tecnología está eliminando puntos únicos de fallo, (9, 18). La blockchain es transparente porque mejora la confianza pública en las investigaciones judiciales, mientras que la interoperabilidad entre instituciones es más fácil con la colaboración entre los sistemas de salud, los laboratorios forenses y los tribunales (26, 30, 36). No obstante, hay otras tecnologías alternativas como RFID o bases de datos relacionales con características específicas, pero la blockchain sobresale por garantizar registros inalterables y que las auditorías sean públicas (12, 30). Sin embargo, la adopción de blockchain a la Medicina Forense, está enfrentando desafíos significativos que se contemplan en la siguiente **Tabla 4:**

**Tabla 4: Retos y Aplicaciones de Blockchain en Medicina Legal y Forense**

| <b>Reto</b>                                  | <b>Descripción</b>  | <b>Ejemplo/Detalle</b>   | <b>Solución Potencial</b>   | <b>Ref.</b>  |
|--|---|--|---|--|
| <b>Seguridad y Auditabilidad</b>             | -Blockchain fortalece la seguridad y auditabilidad de datos.  | -En procesos forenses, los registros inmutables evitan la manipulación de evidencias (por ejemplo, firmas digitales con SHA-256 en criptosistemas RSA/Elgamal).                | -Implementación de los cifrados avanzados:<br>1.CP-ABE,<br>2.Pruebas de conocimiento cero (ZKP)<br>3.Credenciales verificables (VC)<br>-Se mejora la seguridad sin comprometer la privacidad. | 8<br>9<br>12<br>14<br>15<br>18<br>19<br>27<br>28<br>29<br>30<br>33<br>34<br>36 |
|  | -Garantiza la integridad de evidencias forenses y médicas mediante su inmutabilidad (clave para la cadena de custodia en procesos judiciales).  | -En redes públicas, hay riesgo de exposición de los datos.   |   |  |
|  | -La privacidad en blockchains públicas enfrenta complejos retos técnicos y legales.   |  |   |  |
| <b>Interoperabilidad y Colaboración</b>      | -Blockchain facilita la colaboración en investigaciones forenses transfronterizas o en la gestión compartida de datos médicos.  | -El intercambio de datos forenses transfronterizos se agiliza, pero protocolos blockchain diferentes (por ejemplo, Ethereum vs. Hyperledger) generan problemas de integración. | -Desarrollar marcos interoperables que integren blockchain con Identidades Auto-Soberanas (SSI) para un intercambio de datos estandarizado y seguro.  | 8<br>12<br>19<br>27<br>28<br>30<br>36  |
|  | -La falta de estandarización impide una interoperabilidad plena, limitando la aceptación judicial de evidencias almacenadas en blockchain.  |  |   |  |
| <b>Integración de Tecnologías Emergentes</b> | -Integrar blockchain con inteligencia artificial (IA) y el sistema de archivos interplanetario (IPFS).  | -Análisis forense impulsado por IA (por ejemplo, reconocimiento de patrones en forense digital) combinado con IPFS para almacenar grandes conjuntos de datos forenses.         | -Estandarizar protocolos de integración y validar sistemas IA-blockchain mediante pruebas rigurosas para garantizar su aceptación legal.  | 4<br>8<br>12<br>19<br>20<br>23<br>24<br>30                                     |
|  | -La IA permite análisis clínicos y forenses automatizados.<br>-IPFS resuelve necesidades de almacenamiento descentralizado.<br>-Esta integración aumenta la complejidad, complicando la validación técnica y legal. | -La implementación de SSI en forense es limitada.  |   |  |
| <b>Jurisdicción y Legalidad</b>              | -Blockchain facilita el intercambio de datos internacional, pero genera conflictos jurisdiccionales que dificultan la aceptación legal de evidencias almacenadas en la cadena de bloques.                           | -Las evidencias almacenadas en una blockchain global pueden no ser admisibles en tribunales debido a la falta de transparencia jurisdiccional.                                 | -Establecer marcos regulatorios internacionales para estandarizar la admisibilidad de evidencias blockchain.  | 11<br>12<br>27<br>28<br>29<br>34<br>36   |
|  |   |  |   |  |
| <b>Regulación y Cumplimiento de Normas</b>   | -Blockchain tiene potencial para mejorar la trazabilidad cumpliendo con normas.   | -Los registros de pacientes inmutables en blockchain no pueden eliminarse, lo que violaría el derecho al olvido.   | -Desarrollar modelos híbridos de blockchain híbrido con componentes mutables fuera de la cadena para cumplir con regulaciones de privacidad mientras se mantiene la trazabilidad.             | 8<br>9<br>15<br>24<br>26<br>27<br>36<br>37                                     |
|  | -La inmutabilidad choca con regulaciones como GDPR (derecho al olvido) o HIPAA, y las redes descentralizadas generan dudas sobre la responsabilidad legal.  | -La identificación de responsables en redes descentralizadas es complicada.  |   |  |

## 5. CONCLUSIONES

En el área de la Medicina Legal y Forense, la tecnología blockchain ha surgido como un componente transformador para los modelos de seguridad, trazabilidad y transparencia en la gestión de evidencias, la cadena de custodia y la protección de datos. Esta revisión narrativa de un análisis de la literatura científica entre 2017 y 2025, demuestra que blockchain no solo resuelve problemas como la manipulación de evidencias o la falta de interoperabilidad, sino que también abre las posibilidades para que la justicia sea más equitativa, eficiente y confiable. Tenemos el ejemplo del sistema NGO-RMSD en Pakistán, que perfeccionó la gestión de los recursos humanitarios tras un desastre natural, o la combinación de blockchain con tecnologías emergentes como IA en la extracción de evidencias de accidentes de tráfico con un 92.4% de precisión; demostrando que en situaciones reales esta tecnología tiene un gran impacto.

Desde Ethereum a Hyperledger Fabric, las aplicaciones de blockchain, incluyendo las llamadas arquitecturas híbridas con IPFS, están demostrando la capacidad que tiene esta tecnología para dar garantía a la inmutabilidad de los registros, mejorando la auditabilidad y por consecuencia, fomentando la colaboración entre instituciones. Sin embargo, existen retos técnicos (escalabilidad y estandarización), así como, los éticos y legales (como el cumplimiento de normativas como GDPR), donde se exigen soluciones pioneras. Asimismo, se proponen modelos de almacenamiento híbrido, algoritmos de consenso optimizados (PoS, BFT) hasta los frameworks (Polkadot o Cosmos), con el objetivo de que la adopción, de esta tecnología, sea más amplia y efectiva.

Es una realidad que la Blockchain no sólo es una herramienta que está fortaleciendo la confianza pública entre los sistemas judiciales y sanitarios sino que está protegiendo la privacidad de los datos sensibles y acreditando a las instituciones forenses para enfrentar los desafíos del siglo XXI. Este artículo pretende hacer hincapié para que los gobiernos, instituciones académicas y expertos forenses colaboren en la creación de normas globales y que se integre la blockchain con la inteligencia artificial y el IoT.

En el mundo legal, verdad y justicia, dependen de la integridad de los datos y blockchain no es solo una innovación tecnológica, sino un compromiso con un futuro más transparente, resiliente y justo. Adoptar esta tecnología a la Medicina Legal y Forense no es una opción, sino una responsabilidad para garantizar la defensa de los derechos humanos y el estado de derecho. El éxito para ello dependerá de la coordinación entre la innovación tecnológica, la legislación, la viabilidad técnica, la formación continuada de los expertos y los principios éticos. Este es el momento de la actuación y transformación de los sistemas forenses para así construir un legado de confianza y equidad para las generaciones venideras.

### Agradecimientos

Al profesorado del Máster en Formación Permanente en Medicina Forense de la Universidad de Valencia, en especial para el Dr. Fernando Verdú y Dra. Ana Castello por su apoyo académico y motivación en la realización de esta investigación.

### Abreviaturas:

**B-CoC:** Blockchain-based Chain of Custody (Cadena de Custodia basada en Blockchain)

**BFT:** Byzantine Fault Tolerance (Tolerancia a Fallos Bizantinos)

**CoC:** Chain of Custody (Cadena de Custodia)

**EHR:** Electronic Health Record (Registro Electrónico de Salud)

**ETA:** Electronic Transactions Act (Ley de Transacciones Electrónicas)

**GDPR:** General Data Protection Regulation (Reglamento General de Protección de Datos)

**HL7 FHIR:** Health Level Seven Fast Healthcare Interoperability Resources (Recursos de Interoperabilidad Rápida para la Salud)

**HIPAA:** Health Insurance Portability and Accountability Act (Ley de Portabilidad y Responsabilidad de Seguros de Salud)

**IoT:** Internet of Things (Internet de las Cosas)

**IPFS:** InterPlanetary File System (Sistema de Archivos Interplanetario)

**KVKK:** Kişisel Verilerin Korunması Kanunu (Ley Turca de Protección de Datos Personales)

**NGO-RMSD:** Non-Governmental Organization - Rural Medical Services & Development (Organización No Gubernamental - Servicios Médicos Rurales y Desarrollo)

**PoS:** Proof of Stake (Prueba de Participación)

**SIRP:** Security Incident Response Platform (Plataforma de Respuesta a Incidentes de Seguridad)

**YOLOv5:** You Only Look Once version 5 (Algoritmo de detección de objetos basado en aprendizaje profundo)

## REFERENCIAS

1. Calabuig J. Medicina Legal y Toxicología. 7ª ed. Masson. Barcelona, 2004.
2. Beran RG. What is legal medicine – Are legal and forensic medicine the same? Journal of Forensic and Legal Medicine. 2010 Apr;17(3):137–9.
3. Calmon M. Forensic data management and database systems in forensic investigations for cases of missing and unidentified persons in Brazil. Forensic Sci Res. 2023;7(4):599-608. doi:10.1080/20961790.2022.2076994.
4. Al-Rawashdeh M, Keikhosrokiani P, Belaton B, et al. IoT adoption and application for smart healthcare: A systematic review. Sensors. 2022; 22(14):5377. doi:10.3390/s22145377.
5. Loewy AH. Systemic Changes that Could Reduce the Conviction of the Innocent. UNC Legal Studies Research Paper No. 927223. 2006. doi:10.2139/ssrn.927223.
6. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Available from: <https://bitcoin.org/bitcoin.pdf>.
7. Zheng Z, Xie S, Dai H, et al. An overview of blockchain technology: Architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data. IEEE; 2017. p. 557-64. doi:10.1109/BigDataCongress.2017.85.
8. Fonsêca ALA, Barbalho IMP, Fernandes F, et al. Blockchain in Health Information Systems: A Systematic Review. Int J Environ Res Public Health. 2024; 21:1512. doi:10.3390/ijerph21111512.
9. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecomm Policy. 2017;41(10):1027-38. doi: 10.1016/j.telpol.2017.09.003.
10. Sullivan C, Burger E. E-residency and blockchain. Comput Law Secur Rev. 2017;33(4):470-81. doi: 10.1016/j.clsr.2017.03.016.
11. Singapore Law Gazette. Blockchain records under Singapore law. Singapore Law Gazette. Disponible en: <https://lawgazette.com.sg/feature/blockchain-records-under-singapore-law>
12. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telemat Inform. 2019; 36:55-81. doi: 10.1016/j.tele.2018.11.006.
13. Page MJ, McKenzie JE, Bossuyt PM, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ. 2021;372: n71. doi:10.1136/bmj. n71
14. Roman-Belmonte JM, De la Corte-Rodríguez H, Rodríguez-Merchan EC. How blockchain technology can change medicine. Postgrad Med. 2018;130(4):420-427. doi:10.1080/00325481.2018.1472996

15. Okeyinka, A.E., Alao, O., Gbadamosi, B. & Ogundokun, R.O. Application of SHA-256 in formulation of digital signatures of RSA and Elgamal cryptosystems. *International Journal of Information Engineering and Applications*, 2018 ;1(2), pp.61–66.
16. Suryanarayanan, H.G. Digital forensics using blockchain. *International Journal of Recent Technology and Engineering (IJRTE)*, 2019; 8(2S11). <https://doi.org/10.35940/ijrte.B1030.0982S1119>.
17. Litvin, A., Korenev, S.V., Knyazeva, E.G. & Litvin, V. The possibilities of blockchain technology in medicine (Review). *Sovremennye Tehnologii v Medicine*, 2019; 11(4), p.191. Available at: <https://doi.org/10.17691/stm2019.11.4.21>.
18. Li, M., Lal, C., Conti, M. & Hu, D. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Generation Computer Systems*, 2021; 115, pp.406–420. <https://doi.org/10.1016/j.future.2020.09.038>.
19. Indumathi J. Block Chain Forensics: A Systematic Review of the Prospects, *International Journal of Multidisciplinary Research and Modern Education*, 2021; Volume 7, Issue 1, Page Number 26-36. <http://doi.org/10.5281/zenodo.5008556>
20. Olukoya, O. Distilling blockchain requirements for digital investigation platforms. *Journal of Information Security and Applications*, 2021; 62, p.102969. Available at: <https://doi.org/10.1016/j.jisa.2021.102969>.
21. Tsai, F.-C. The application of blockchain of custody in criminal investigation process. *Procedia Computer Science*, 2021; 192, pp.2779–2788. Available at: <https://doi.org/10.1016/j.procs.2021.09.048>.
22. Ozkan, Arzu and Korkmaz, Umutcan and Dak, Cemal and Karaarslan, Enis. A Decentralized Resource Management System Proposal For Disasters: NGO-RMSD (STK-AKYS), 2022. Available at SSRN: <https://ssrn.com/abstract=4171468> or <http://dx.doi.org/10.2139/ssrn.4171468>
23. Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet*, 2022; 14(11), 341. <https://doi.org/10.3390/fi14110341>
24. Adere EM. Blockchain in healthcare and IoT: A systematic literature review. *Array*. 2022; 14:100139. doi: 10.1016/j.array.2022.100139
25. Ortiz-Lizcano, M.I., Arias-Antunez, E., Hernández Bravo, Á., Caminero, M.B., Rojo Guillen, T. & Nam Cha, S.H. Increasing the security and traceability of biological samples in biobanks by blockchain technology. *Computer Methods and Programs in Biomedicine*, 2023; 231, p.107379. Available: <https://doi.org/10.1016/j.cmpb.2023.107379>.
26. Reegu, F.A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A.A., Jabbari, A., Sonkamble, R.G. & Dziauddin, R.A. (2023) Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability*, 15(8), p.6337. Available at: <https://doi.org/10.3390/su15086337>.
27. D'Anna, T., Puntarello, M., Cannella, G., 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 (Basel)*, 2023; 11(5), p.634. Available at: <https://doi.org/10.3390/healthcare11050634>.
28. Batista, D., Mangeth, A.L., Frajhof, I., Alves, P.H., Nasser, R., Robichez, G., Silva, G.M. & Miranda, F.P.d. Exploring blockchain technology for chain of custody control in physical evidence: A systematic literature review. *Journal of Risk and Financial Management*, 2023; 16(8), p.360. Available at: <https://doi.org/10.3390/jrfm16080360>.
29. Liu, S. & Zheng, Q. A study of a blockchain-based judicial evidence preservation scheme. *Blockchain: Research and Applications*, 2024; 5(2), p.100192. Available at: <https://doi.org/10.1016/j.bcra.2024.100192>.

30. Atlam HF, Ekuri N, Azad MA, Lallie HS. Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. *Electronics*; 2024; 13(17):3568. <https://doi.org/10.3390/electronics13173568>
31. Fan Wei et al. Blockchain digital forensics: technology and architecture. *Tongxin Xuebao*. 2024; 45124–141. DOI : [10.11959/j.issn.1000-436x.2024204](https://doi.org/10.11959/j.issn.1000-436x.2024204)
32. Ffaizal, A. and Luthfi, A. Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis, *Journal of Information Systems and Informatics*, 2024; 6(2), pp. 701-718. doi: 10.51519/journalisi. v6i2.717.
33. Patil, H., Kohli, R.K., Puri, S. & Puri, P. Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework. *Egyptian Journal of Forensic Sciences*, 2024; 14(1). Available at: <https://doi.org/10.1186/s41935-023-00383-w>.
34. Su, Z. Evidentiary value and evidentiary status of blockchain evidence. *The International Journal of Evidence & Proof*, 2024; 29(1), 58-76. <https://doi.org/10.1177/13657127241238020>
35. An, Q., Zhao, Y., Yu, M., Sa, R., Gao, Q., Zhang, J. Blockchain-Based Traffic Accident Evidence Management Scheme. In: Sun, H., et al. *Computer Supported Cooperative Work and Social Computing. ChineseCSCW 2024. Communications in Computer and Information Science*, 2025; vol 2343. Springer, Singapore. [https://doi.org/10.1007/978-981-96-2373-0\\_6](https://doi.org/10.1007/978-981-96-2373-0_6)
36. Loffi, L., Camillo, G.L., De Souza, C.A., Westphall, C.M. & Westphall, C.B. Management of the chain of custody of digital evidence using blockchain and self-sovereign identities: a systematic literature review. *IEEE Access*, 2025;13, pp.77804–77832. doi:10.1109/ACCESS.2025.3560191.
37. Vaishali R, Vijayakanthan G. Blockchain Technology in Healthcare: A Systematic Review with a Focus on Sri Lanka. *J Inf Commun Technol*. 2025;2(Spec Issue):64-70. Disponible en: <https://www.seu.ac.lk/jict/publication/v2s1/64-70%20Blockchain.pdf>