Vox Juris – Vol. 44 – N° 2 – Julio – Diciembre – 2026 – ISSN 1812-6804 / 2521-5280 – Páginas: 105-118

PERSPECTIVAS PRELIMINARES SOBRE LA CADENA DE CUSTODIA EN LA EVIDENCIA DIGITAL MEDIANTE EL USO DE *BLOCKCHAIN*

PRELIMINARY PERSPECTIVES ON THE CHAIN OF CUSTODY FOR DIGITAL EVIDENCE USING BLOCKCHAIN

Eduardo Andrés Calderón Marenco*

Yonni Albeiro Bermúdez Bermúdez**

Universidad Cooperativa

Colombia

Gabriel Ravelo-Franco***

Universidad Continental

Perú

Recibido: 14 de agosto del 2025 **Aprobado:** 10 de octubre del 2025

RESUMEN

El artículo examina la cadena de custodia como sistema normativo–técnico que garantiza identidad, integridad y autenticidad de la evidencia, y propone su actualización frente a la evidencia digital. Sostiene que la cadena opera en dos planos, formal (documentación continua) y material (conservación efectiva), y que, en entornos digitales, requiere mismidad a nivel de bits mediante adquisición forense bit a bit, preservación de metadatos, funciones hash y sellos de tiempo. Metodológicamente, se emplea un enfoque cualitativo de análisis documental y revisión de literatura especializada, incluidos estudios sistemáticos y estándares forenses, para construir un marco comparado y aplicable. En el cuerpo del trabajo se distinguen las particularidades probatorias de documentos digitales, la necesidad de protocolos y capacitación, y la integración de tecnologías descentralizadas. Se argumenta que blockchain aporta una capa complementaria de sellado temporal, trazabilidad y verificación independiente,siempre con contenido probatorio fuera de cadena, gobernanza de claves, control de accesos y respeto estricto de licitud y pericia. El marco propuesto prioriza minimización de datos anclados, redes permisionadas o híbridas, interoperabilidad con estándares, pruebas reproducibles y validaciones empíricas. Se concluye que blockchain no reemplaza la metodología forense ni las garantías procesales, pero refuerza la cadena de custodia cuando se inserta en un flujo previamente validado, permitiendo auditoría extrema a extremo y mejora la confianza probatoria sin resolver por sí misma los problemas de atribución, privacidad y coordinación transfronteriza.

Palabras clave: trazabilidad probatoria; sellado temporal; integridad; pericia informática; interoperabilidad forense.

ABSTRACT

The article examines the chain of custody as a normative–technical system that guarantees the identity, integrity, and authenticity of evidence, and proposes its updating for digital evidence. It argues that the chain operates on two planes—formal (continuous documentation) and material (effective preservation)—and that, in digital settings, it requires bit-level identity through bit-by-bit forensic acquisition, metadata preservation,

Para citar este artículo: Calderón Marenco, E. A., Bermúdez Bermúdez, Y. A., & Ravelo-Franco, G. (2026). Perspectivas preliminares sobre la cadena de custodia en la evidencia digital mediante el uso de blockchain. *Vox Juris*, 44(2), [pp. 105–118]. DOI: https://doi.org/ [DOI-asignado]

* Eduardo Andrés Calderón Marenco. Doctor en Derecho. Universidad Cooperativa de Colombia. ORCID 0000-0002-7840-6495. Correo: eduardo.calderon@campusucc.edu.co

** Yonni Albeiro Bermúdez Bermúdez. Magíster en Procedimiento Penal. Universidad Cooperativa de Colombia. ORCID 0000-0001-8766-6953. Correo: yonni.bermudez@campusucc.edu.co

*** Gabriel Ravelo-Franco. Maestro en Derecho Penal. Universidad Continental, Perú. ORCID 0000-0003-0212-312X. Correo: gravelo@continental.edu.pe

hash functions, and trusted timestamps. Methodologically, it adopts a qualitative approach based on documentary analysis and a review of specialized literature—including systematic studies and forensic standards—to build a comparative, applicable framework. The body of the work distinguishes the probative particularities of digital documents, the need for protocols and training, and the integration of decentralized technologies. It contends that blockchain adds a complementary layer of timestamping, traceability, and independent verification, with probative content kept off-chain, robust key governance, access control, and strict compliance with lawfulness and expert examination. The proposed framework prioritizes minimal anchoring of data, permissioned or hybrid networks, interoperability with standards, reproducible tests, and empirical validation. It concludes that blockchain does not replace forensic methodology or procedural guarantees; rather, it strengthens the chain of custody when embedded in a previously validated workflow, enabling end-to-end auditability and improving probative confidence without, by itself, resolving challenges of attribution, privacy, and cross-border coordination.

Keywords: *evidentiary traceability; trusted timestamping; data integrity; digital forensic expertise; forensic interoperability.*

SUMARIO

I. Introducción. II. Consideraciones sobre la prueba digital y la cadena de custodia tecnológica. III. Aplicación de tecnologías descentralizadas a la cadena de custodia. IV. Conclusiones. V. Bibliografía.

INTRODUCCIÓN

La expansión de los entornos digitales ha multiplicado la generación, transmisión y almacenamiento de información con potencial probatorio. En ese ámbito, la cadena de custodia, concebida históricamente para evidencias físicas, enfrenta tensiones derivadas de la volatilidad de los datos, la facilidad de copia y manipulación, la dependencia de metadatos y la creciente heterogeneidad de dispositivos y servicios. La doctrina y la práctica forense coinciden en que la fiabilidad del itinerario probatorio exige procedimientos de adquisición *bit a bit*, preservación de metadatos y controles de integridad verificables, pero persisten asimetrías operativas y vacíos metodológicos que dificultan la trazabilidad completa desde el hallazgo hasta la valoración judicial.

Esta investigación se justifica por la necesidad de actualizar el concepto y la praxis de la cadena de custodia frente a la evidencia digital y por el interés en evaluar el aporte específico de las tecnologías descentralizadas como capa de sellado temporal, trazabilidad y verificación independiente. El propósito es fortalecer la confianza probatoria sin alterar las garantías del debido proceso ni sustituir la pericia, integrando soluciones técnicas con criterios jurídicos y organizacionales.

El problema que guía la investigación se formula en términos de condiciones y límites ¿cómo garantizar identidad, integridad y autenticidad de la evidencia digital a lo largo de todo su ciclo de vida? y ¿bajo qué supuestos resulta pertinente incorporar *blockchain* sin comprometer licitud, privacidad y gobernanza? En otras palabras, se indaga si es posible articular un marco técnicamente sólido y jurídicamente compatible que permita anclar huellas y metadatos indispensables, manteniendo el contenido probatorio fuera de cadena y asegurando interoperabilidad con estándares forenses.

El objetivo general es examinar la cadena de custodia de evidencia digital y proponer un marco de adopción de *blockchain* que refuerce su fiabilidad. De manera complementaria, se busca precisar el concepto y los elementos sustanciales de la cadena de custodia en clave digital, identificar riesgos y salvaguardas asociados a la obtención, conservación, análisis y presentación de datos, analizar el funcionamiento técnico de las tecnologías descentralizadas con foco en su valor probatorio y derivar criterios de diseño, gobernanza y evaluación que orienten implementaciones responsables, incluyendo un ejemplo aplicado.

Metodológicamente, se adopta una investigación teórica enfoque cualitativo. Se adopt**ó** el método de análisis–síntesis. En la fase de análisis, descompone cada fuente en sus elementos esenciales (conceptos, supuestos, variables técnicas y criterios jurídicos) para identificar convergencias y discrepancias en torno a cadena de custodia digital y uso de *blockchain*. En la fase de síntesis, integra esos hallazgos en un marco coherente que articula definiciones, requisitos funcionales, arquitectura tecnológica y lineamientos operativos, con el fin de proponer un modelo aplicable sin contrariar las garantías procesales.

La técnica de búsqueda de información se apoy**ó** en bases de datos especializadas —SciELO, Biblat, JSTOR, Scopus, Dialnet y Web of Science—, con estrategias combinadas en español e inglés. Se emplean descriptores y operadores booleanos ajustados al objeto de estudio: "cadena de custodia digital", "prueba digital", "evidencia electrónica", "blockchain AND chain of custody", "digital forensics AND blockchain", "hash AND timestamp", "proveniencia probatoria", "forensic readiness", "permissioned blockchain", "IoT forensics", "Merkle tree", "Lex Criptográfica", "integridad AND autenticidad", "auditabilidad AND evidencia". Los resultados pasan por filtros de pertinencia temática y calidad académica hasta conformar un corpus de 27 documentos que el artículo cita y referencia.

El instrumento de recolección consistió en una ficha bibliográfica de diseño propio para cada obra, con campos que capturan datos de identificación, objeto, método, estándares técnicos citados, aportes al concepto y a las fases de la cadena de custodia, propuesta tecnológica, limitaciones y conclusiones relevantes. La aplicación uniforme de la ficha asegur**ó** trazabilidad del proceso de revisión y permitió comparar enfoques doctrinales y tecnológicos bajo criterios homogéneos, condición necesaria para la posterior síntesis y la formulación del marco de adopción.

Se anticipa como conclusión que *blockchain* no reemplaza la metodología forense ni las garantías procesales, pero puede reforzarlas como línea de tiempo probatoria verificable por terceros, siempre que el anclaje se realice sobre adquisiciones forenses válidas, que el contenido permanezca fuera de cadena bajo custodia pericial, que exista gobernanza robusta de identidades y claves, y que se asegure interoperabilidad con estándares y auditorías reproducibles. Bajo estas condiciones, la adopción responsable mejora la trazabilidad y la auditabilidad sin resolver por sí misma los retos de atribución, privacidad y coordinación transfronteriza, que requieren políticas y procedimientos complementarios.

II. CONSIDERACIONES SOBRE LA PRUEBA DIGITAL Y LA CADENA DE CUSTODIA TECNOLÓGICA

1. Semblantes conceptuales sobre la prueba digital

El término evidencia, a partir de una concepción amplia, se define como cualquier elemento, dato o información que ostenta certeza clara y manifiesta de la que no se puede dudar (RAE, 2024). En contextos legales, esta adquiere un rol fundamental que permite proporcionar fundamentos objetivos a los tribunales para lograr un adecuado análisis para la posterior toma de decisiones. Ahora bien, el rol que se le ha atribuido en los contextos legales no radica solo en su existencia física, sino que se debe partir de su calidad, relevancia y credibilidad, es decir, estos aspectos son los que deben ser objeto de valoración para lograr determinar su capacidad de influir en los resultados de un proceso o investigación.

En este sentido, la evidencia ha venido presentando una constante evolución, es así como, de la evidencia física hoy en día se habla de la evidencia digital. La primera de estas evidencias hace referencia a todos aquellos elementos tangibles a través de los cuales se logra objetivizar una observación (Sánchez Prada & Mora Izquierdo, 2001). Es decir, son objetos materiales que se encuentran relacionados con un hecho ilícito, puesto que son utilizados como instrumentos o son el fruto de este, de ahí que, tienen la capacidad de lograr dejar huella en el mundo exterior (González et al., 2021). Estas evidencias físicas se pueden encontrar en el lugar de los hechos en diferentes estados a saber: liquido, gaseoso y sólido.

En cuanto a la evidencia digital esta se ha definido como aquella información que tiene un valor probatorio la cual se encuentra almacenada o es transmitida de forma digital (Ochoa Arévalo, 2018). Entonces, este tipo de evidencia está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales (Cruz Vela, 2014). Asimismo, se caracteriza por ser intangible ya que tiene una dependencia directa de los medios tecnológicos. También, se le reconoce su carácter dinámico y volátil lo cual hace necesario que la intervención que se realice sobre este tipo de evidencia sea cuidadosamente planificada y ejecutada bajo protocolos adecuados que permitan un manejo correcto con el cual se logre garantizar su integridad y autenticidad.

El estudio y manejo adecuado de la evidencia física se convierte en un pilar fundamental para garantizar transparencia, veracidad y acceso a la administración de justicia. El reciente auge de la evidencia digital ha demandado que la criminalística tradicional adopte una rama dedica al estudio de este evidencia, es así como aparece la informática forense, la cual se encarga de emplear métodos y técnicas científicas aprobadas por la comunidad internacional, con las cuales se logra identificar, preservar, validar, analizar, interpretar y documentar la evidencia digital, con el propósito de facilitar la reconstrucción de hechos en una investigación judicial, o ayudar a anticipar o prevenir acciones ilícitas que vayan en contra de la ley (Monti & Martínez, 2023).

De esta forma a la evidencia digital se le han reconocido una serie de principios que debe cumplir para lograr ser incorporada en debida forma dentro de un proceso judicial, a saber: (i) admisible, (ii) auténtica, (iii) completa, (iv) confiable y (v) creíble (Ochoa Arévalo, 2018). La admisibilidad hace referencia a que la evidencia debe lograrse incorporar al proceso judicial, es decir, para que pueda un elemento, dato o información considerado como una evidencia admisible debe ser objeto de valoración por parte de un tribunal. En cuanto a la autenticidad esta debe ser real, es decir, no debe ser una evidencia que haya sido alterada o suplantada de manera voluntaria o por imprudencia en el manejo de esta evidencia.

La evidencia debe ser completa, esto significa que debe tener un alto potencial de lograr demostrar una perspectiva integral del hecho ilícito, de ahí que, tenga la suficiente capacidad de lograr probar las acciones o inocencia de los investigados en el proceso judicial. Aunado a lo anterior, se le reconoce como principio de la evidencia digital que esta debe ser confiable, esto quiere decir, que cuando se identifica, recolecta y se analiza no debe existir duda sobre su veracidad. Por lo tanto, es este el principio que más se ataca de la evidencia digital, pues al momento de su manejo pueden presentarse indebidas manipulaciones que logren afectar la autenticidad de la evidencia, lo cual permita afirmar que a pesar de existir la evidencia esta no podrá ser incorporada al proceso judicial por defectos en su manejo.

En relación con la credibilidad se destaca que la evidencia digital debe gozar de claridad, esto repercute en que debe ser entendible y convincente para un tribunal, de manera que pueda ser utilizada de forma efectiva en un proceso judicial para soportar una decisión. Ahora bien, los principios que deben regir la evidencia digital se han logrado poner en tela de juicio como consecuencia de nuevas técnicas antiforense que están en la capacidad de destruir, ocultar, eliminar o falsificar la evidencia digital (Contreras Calderón, 2021). Esto sin lugar a duda genera nuevos retos para el correcto manejo de la evidencia digital, toda vez que, se deben emplear mejores técnicas de investigación que permitan hacer frente a estas nuevas realidades.

Además de los elementos intrínsecos antes señalados, la evidencia digital debe cumplir con unos elementos extrínsecos, a saber: (i) claridad, (ii) autenticidad, iii) integridad iv) y licitud (Bujosa Vadell et al., 2021). En cuanto al primer elemento, este se subdivide en dos momentos claves, su proceso de obtención y estudio. El primer momento hace referencia a que se deben cumplir con todos los requisitos legales al momento de obtener la evidencia digital, esto es aplicar el procedimiento adecuado conforme al medio de prueba identificado. Asimismo, es necesario que aquellas personas que entran en contacto con la evidencia digital al momento de su estudio cuenten con los elementos idóneos para su manejo y posterior estudio, pues un manejo inadecuado o falta de pericia tiene como consecuencia que la evidencia digital se altere y pierda sus elementos intrínsecos.

En cuando a la licitud como requisito extrínseco de la evidencia digital resulta trascendental para que el medio de prueba pueda ser valorado en el proceso que se haya obtenido sin el desconocimiento de derechos fundamentales, esto es: debido proceso, intimidad, defensa, etc. De verse afectado alguno de los anteriores requisitos extrínsecos, la evidencia digital carecería de valor para ser aportada al proceso judicial, lo cual repercute de manera directa con el resultado de este.

En términos prácticos, se recomienda garantizar desde el procedimiento de obtención y su posterior presentación como medio de prueba en el escenario judicial que se garanticen las características únicas de la evidencia digital obtenida, a través de un adecuado control y manejo en el protocolo de cadena de custodia. Este método se conoce como huella digital o *hash* o *hashing* (Baracaldo-Lozano & Daza-Giraldo, 2015). Así, el protocolo de cadena de custodio que se emplea para la preservación de la evidencia digital hoy en día ocupa uno de los roles más importantes dentro del proceso penal, puesto que debe evitar a toda costa que el medio de prueba sea alterado o manipulado.

2. Acerca de la cadena de custodia

La cadena de custodia se concibe como una garantía del derecho a la prueba con dos planos: uno formal (o procesal), que asegura la mismidad —equivalencia procesal entre lo obtenido y lo presentado— mediante la "corrección" de la cadena, y otro material, que abarca los actos desde la aprehensión de la fuente hasta su incorporación al juicio por el medio probatorio idóneo. la autora subraya la orfandad normativa y el papel homogeneizador de la jurisprudencia, así como la influencia de protocolos y guías institucionales en la praxis. en evidencia tecnológica, matiza la presunción clásica: ante impugnación, debe acreditarse autenticidad e integridad (a menudo vía pericia informática), pues la facilidad de manipulación impacta la fiabilidad. además, sitúa a las tecnologías disruptivas —en especial *blockchain*— como soporte preventivo para probar identidad e inalterabilidad mediante encadenamiento de *hashes*, facilitando la verificación de cualquier alteración. (Jamardo Lorenzo, 2025).

Igualmente puede indicarse que a partir de la cadena de custodia se define como un procedimiento controlado que acompaña a los indicios materiales desde su localización en el sitio del suceso hasta su valoración judicial, con la finalidad de evitar alteración, sustitución, contaminación o destrucción y así preservar integridad y autenticidad probatoria. esta concepción se operacionaliza mediante actuaciones secuenciales en criminalística de campo —aseguramiento y fijación del lugar, identificación, recolección, embalaje, rotulado, transporte, almacenamiento y peritaje— documentadas en la planilla de registro y guiadas por el manual único de cadena de custodia de evidencias físicas y protocolos complementarios (Vacaro Bolívar, 2025). Arellano y Castañeda (2012) la describen como un procedimiento controlado que abarca desde la localización del indicio hasta su estimación final, evitando alteraciones o contaminaciones.

Así las cosas, Guevara y Mora (2025) conciben la cadena de custodia como una garantía procesal que preserva integridad, autenticidad y legalidad de los indicios desde su recolección hasta su valoración judicial. El fundamento de este proceso se sitúa en el derecho al debido proceso, por lo que interrupciones, errores u omisiones en cualquier fase —fijación, levantamiento, embalaje, rotulado, transporte, almacenamiento y análisis— erosionan la trazabilidad y habilitan exclusión probatoria, nulidades y afectación de imparcialidad. En este sentido, es claro que la cadena de custodia trasciende lo técnico y opera como pilar de legitimidad del proceso penal.

Por su parte, Ovelar (2024) entiende a la cadena de custodia como un sistema normativo-técnico de control y documentación continua que acompaña a los indicios desde su descubrimiento hasta su disposición final, con el propósito de garantizar su identidad, integridad y autenticidad mediante un registro exhaustivo de sujetos, tiempos, lugares y cambios efectuados. Conceptualmente, opera como un procedimiento que describe momentos y circunstancias de contacto con la evidencia; además, un régimen de principios —legalidad, identidad, integridad, preservación, seguridad y registro— que orienta la ejecución; y un mecanismo de trazabilidad que asegura que lo presentado en juicio sea el mismo objeto fijado, recolectado, embalado y trasladado desde la escena. Así

entendida, la cadena no es una mera formalidad probatoria, sino la condición de posibilidad de la fiabilidad del medio de prueba, pues evita sustituciones, contaminaciones o alteraciones que comprometan la decisión jurisdiccional y la seguridad jurídica del proceso penal.

En suma, la cadena de custodia es un sistema normativo-técnico de trazabilidad probatoria que funciona, a la vez, como garantía y como procedimiento. Su finalidad es asegurar identidad, integridad y autenticidad mediante un registro continuo y verificable de personas, tiempos, lugares y acciones que intervienen sobre la evidencia. El sistema opera en dos planos: uno formal, que exige la corrección documentada de cada transferencia, y otro material, que demanda conservación efectiva de la fuente hasta su incorporación procesal. Una ruptura no determina por sí sola la nulidad, pero impone escrutinio reforzado y puede justificar exclusión si la fiabilidad queda comprometida. La estandarización protocolaria y la conducción institucional reducen asimetrías operativas y fortalecen la legitimidad del proceso. Con este núcleo conceptual, el siguiente paso a revisar es la cadena de custodia tecnológica, un marco que extiende dichos principios al nivel de bits para garantizar la fiabilidad de la prueba digital. Y es que, tratándose de evidencia digital, se tiene la necesidad de una cadena de custodia digital que asegure integridad y trazabilidad desde la obtención y conservación de datos hasta su incorporación y valoración judicial, dadas su volatilidad y susceptibilidad de manipulación.

3. Nuevas tecnologías y la cadena de custodia

En clave tecnológica, la cadena de custodia se reconfigura como un régimen bifronte, una vertiente formal, estática, orientada a acreditar la mismidad mediante la corrección documentada del itinerario probatorio; y una vertiente material, dinámica, que adapta actos de hallazgo, aseguramiento, conservación, análisis e incorporación al juicio según la naturaleza digital de la fuente. Este tránsito enfrenta dos tensiones, la primera de ellas, orfandad normativa (falta de regulación procesal unitaria, suplantada por protocolos y guías institucionales), y la segunda, desconfianza epistémica hacia la prueba digital por volatilidad, replicabilidad y facilidad de manipulación. Existen algunos avances en los ordenamientos jurídicos nacionales, por ejemplo, el marco español incorpora, además, restricciones propias de la investigación tecnológica (especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad), que condicionan la preservación y el acceso a datos. En ese tejido, la pericia informática, los fedatarios en momentos críticos de acceso/clonado y, como técnica complementaria, el uso de hashes y registros inmutables (verbigracia, *blockchain*) operan como vías para reforzar identidad e integridad sin desplazar la valoración judicial, cuestiones que se abordarán más adelante (Jamardo Lorenzo, 2024).

Ahora bien, bajo los principios de equivalencia funcional y no discriminación de soportes, lo determinante deja de ser la hoja de ruta y pasa a ser el soporte y el procedimiento técnico. Para mantener la trazabilidad e integridad, se exige trabajar con el documento digital original (o imagen forense *bit* a *bit*) y no con meras representaciones impresas o capturas, pues solo el primero preserva metadatos auditables y habilita verificación pericial; ello implica identificar origen, cadena de transferencias, control de acceso y parámetros de conservación segura (Busso, 2024).

Al respecto de los derechos fundamentales, la digitalización obliga a replantear la cadena de custodia desde la distinción entre fuente y medio de prueba: la primera es la información creada, almacenada o transmitida electrónicamente; el segundo, la vía procesal de incorporación al expediente. Esta distinción tiene consecuencias operativas: la trazabilidad debe documentar cada acceso, copia, transferencia y tratamiento técnico desde la obtención hasta la valoración judicial, con registros verificables que aseguren identidad, integridad y autenticidad. Al mismo tiempo, la custodia de datos y dispositivos incide directamente en la intimidad, el secreto de las comunicaciones, la inviolabilidad domiciliaria y la autodeterminación informativa, por lo que toda medida tecnológica requiere parámetros de jurisdiccionalidad, necesidad y proporcionalidad, y un diseño de gobernanza documental (control de accesos, bitácoras, sellos de tiempo, auditoría) que minimice los riesgos de afectación a derechos. La jurisprudencia conecta además la ruptura de la cadena con problemas de fiabilidad de la prueba —no

necesariamente de licitud—, de modo que la eventual fractura puede expulsar elementos de cargo, pero no vicia per se el conjunto si existen otras fuentes independientes que acrediten autenticidad (González Granda & Ariza Colmenarejo, 2021).

En este orden de ideas, es claro se hace toral que existan mecanismos que permitan una mayor fiabilidad del manejo de la prueba digital mediante la cadena de custodia, es así que, según López Jiménez (2021), la verificación de que la información no ha sido manipulada descansa en procedimientos técnicos de adquisición y control que permiten contrastar la mismidad entre lo obtenido y lo que se presenta al juzgador. El eje es la copia *bit a bit* (imagen forense), que clona el contenido a nivel de *bits* —no el soporte— y traslada el examen a las copias de trabajo, manteniendo incólume el original. Esta técnica posibilita, además, la recuperación de eliminados y la comparación determinista mediante funciones *hash* calculadas antes y después de cada intervención para detectar cualquier alteración. Además, que lo borrado deja huella digital analizable y que, por la facilidad de manipulación y de edición de metadatos, resulta imprescindible documentar herramientas, parámetros y responsables, y apoyar la autenticidad con pericia informática.

Agrega López Jiménez (2021) que, complementariamente, los algoritmos de verificación (funciones de resumen) se utilizan para acreditar integridad con mayor eficiencia en archivos voluminosos, operando como comprobación independiente de inalterabilidad. La metodología recomendada combina, adquisición forense *bit a bit*; cálculo y recalculado de sumas criptográficas en cada transferencia; trabajo exclusivo sobre duplicados; y trazabilidad documental de accesos y transferencias, pudiendo incluir la custodia de una copia maestra y la intervención de fedatarios u otros mecanismos que fortalezcan la cadena. En conjunto, estos procedimientos constituyen un sistema verificable y repetible que reduce incertidumbre técnica y soporta la valoración judicial sobre autenticidad e integridad de la evidencia, lo que no implica que puedan analizarse la introducción de otras tecnologías.

En suma, la aplicación de tecnologías a la cadena de custodia exige un andamiaje forense completo desde la obtención hasta la presentación del material, duplicación *bit a bit* certificada; cálculo y verificación de sumas criptográficas (MD5/SHA) antes y después de cada intervención; preservación de metadatos; registro pormenorizado de herramientas, versiones, parámetros y responsables; almacenamiento en contenedores con evidencia de apertura; y segregación de funciones para evitar conflictos. Este esquema favorece la reproducibilidad del examen técnico y permite detectar cualquier modificación del contenido. En entornos conectados, la atribución también requiere correlacionar direcciones IP con historiales de red y datos de proveedores, lo que impone políticas claras de conservación y solicitud de información técnica. (López Jiménez, 2021).

Por último, en este marco, sin lugar a duda pueden tenerse en cuenta soluciones de registro inmutable, las que podrían desempeñar un papel complementario para reforzar la cadena de custodia digital. La propuesta de asignar a una institución la administración de un sistema basado en *blockchain* —empleado, por ejemplo, en protocolos de protección de secreto empresarial para controlar accesos y preservar evidencias— ilustra un modelo en el que la red distribuida aporta trazabilidad y transparencia sobre quién accede, cuándo y con qué permisos, sin sustituir la pericia ni las garantías procesales. La utilidad probatoria se apoya en funciones *hash* y sellado temporal para acreditar inalterabilidad y detectar cualquier modificación *bit a bit*, integrándose como capa de aseguramiento que facilita la verificación de la mismidad entre la fuente digital y el medio ofrecido en juicio. La clave, sin embargo, sigue siendo regulatoria y organizacional, sin reglas claras y supervisión judicial, la tecnología no reemplaza los estándares de licitud ni la evaluación estricta de compatibilidad con derechos fundamentales (González Granda & Ariza Colmenarejo, 2021). En este sentido se procederá a realizar una exposición argumentativa sobre un posible marco para la implementación de tecnologías descentralizadas en la cadena de custodia.

III. APLICACIÓN DE TECNOLOGÍAS DESCENTRALIZADAS A LA CADENA DE CUSTODIA

1. Tecnologías descentralizadas ¿cómo funcionan?

Puede afirmarse que las tecnologías descentralizadas operan sobre un libro mayor distribuido cuya integridad se asegura combinando criptografía y consenso. Cada evento se representa mediante funciones *hash* y estructuras encadenadas que vuelven detectable cualquier alteración; la replicación en múltiples nodos evita puntos únicos de fallo y habilita verificación independiente. La consensuación (tolerante a fallos bizantinos) determina qué bloques se incorporan, produciendo un efecto de inmutabilidad práctica y sellado temporal. Sobre esa base, los contratos inteligentes añaden una máquina de estados compartida que ejecuta reglas programadas y verificables por todos los participantes, generando un rastro auditable de quién hizo qué y cuándo sin acudir a un custodio único. En suma, la tríada código–criptografía–registro distribuido explica el funcionamiento técnico que, luego, permite diseñar casos de uso probatorios (anclaje de huellas, trazabilidad de transferencias y auditoría de accesos) (Calderón Marenco et al., 2024).

Es importante agregar que a la tecnología de *blockchain* pueden sumarse estructuras como los *árboles de Merkle* permiten verificar con eficiencia la pertenencia de un elemento al conjunto sin reconstituir todo el registro, mientras que las firmas digitales garantizan autenticación y no repudio de los participantes. De esta forma, el sistema ofrece verificación independiente por terceros sin necesidad de un custodio único, y un historial auditable de cambios en el tiempo. Desde una perspectiva de diseño, las redes públicas priorizan apertura y resistencia a la censura, mientras que las permisionadas acotan el acceso y la validación para optimizar rendimiento y cumplimiento. En ambos modelos, la seguridad deriva de la combinación entre criptografía, distribución y consenso, que encarece los intentos de reescritura retrospectiva y facilita auditorías *ex post* (Calderón Marenco et al., 2025). Para fines probatorios, esta arquitectura permite pruebas de existencia en fecha cierta, verificación de integridad mediante huellas digitales y trazabilidad de eventos relevantes, habilitando el anclaje de evidencias y el seguimiento de transferencias sin desplazar los controles de licitud ni la pericia forense.

A modo ilustrativo, en una red permisionada que interconecta laboratorio forense, policía judicial y fiscalía, un contrato inteligente denominado *RegistroCustodia* exige que toda transferencia de evidencia se inscriba con: el identificador único del elemento probatorio; la huella criptográfica de la imagen forense (*hash* del archivo maestro); el rol e identidad digital del responsable de la entrega o recepción; y la referencia al eslabón inmediatamente anterior. El propio contrato verifica que quien firma esté autorizado, que la nueva anotación se encadene al último estado válido y que no existan solapamientos temporales; cualquier intento de registrar una operación fuera de secuencia, con un *hash* incongruente o por un actor sin permisos se rechaza automáticamente por las reglas de la red. La auditoría se realiza contrastando el *hash* del expediente conservado en almacenamiento fuera de línea (cadena fría) con el registrado en la red y obteniendo pruebas de pertenencia mediante *árboles de Merkle* y marcas de tiempo del bloque. El resultado es un rastro cronológico, prácticamente inmutable, que refuerza identidad, integridad y autenticidad sin sustituir la pericia forense ni los controles de licitud en la obtención.

En este sentido, *blockchain* se perfila como un soporte idóneo para la conservación y trazabilidad de evidencia electrónica en ámbitos transfronterizos, dado de que su naturaleza distribuida permite registrar eventos con fecha cierta y verificación independiente, aportando un rastro estable de quién hizo qué y cuándo. En temas normativos, Europa y su derecho comunitario está a la vanguardia, dado que el Reglamento (UE) 2023/1543 abre la puerta a sistemas informáticos descentralizados como canal seguro para custodiar datos obtenidos mediante órdenes europeas de producción o de conservación; *blockchain* encaja técnicamente en ese rol, aunque persiste una laguna procesal sobre el medio de incorporación al proceso penal (documental, pericial u otros), distinción clave entre fuente y medio de prueba.

2. Marco para la adopción de *blockchain* en la cadena de custodia

Desde el ángulo técnico-probatorio, el valor de *blockchain* descansa en tres atributos, seguridad (encadenamiento de *hashes* y firmas digitales que vuelve detectable cualquier alteración retrospectiva), transparencia (libro mayor consultable y protocolos abiertos, con matices sobre la pseudonimidad de usuarios) e inmutabilidad práctica (replicación y consenso que fijan estados y sellos temporales). Estos rasgos justifican su uso para pruebas de existencia, verificación de integridad y cronología fiable de eventos relevantes. Ahora bien, su encaje procesal actual se articula, preferentemente, como documento electrónico privado acompañado de pericia informática que traduzca el *hash* y acredite la correspondencia con el dato subyacente; la jurisprudencia admite su aportación con garantías, pero no lo equipara al documento público salvo reforma legislativa. Para el propósito de cadena de custodia, su aportación es clara, ofrecer verificabilidad externa (pruebas de existencia y no alteración en tiempo cierto) sin sustituir la licitud de la obtención ni la valoración pericial, sino complementándolas con evidencias criptográficas y trazabilidad pública o permisionada, según el diseño de la red.

La incorporación de *blockchain* debe partir de una premisa técnica clara como lo es el anclaje en un registro distribuido no certifica la veracidad del contenido, sino la existencia y fijación de su integridad en un momento concreto. Si la huella se calcula sobre material ya alterado o degradado, lo que se inmoviliza es la falsificación con la misma fuerza que el original. Por ello, el flujo previo es determinante, adquisición *bit a bit* del soporte original, preservación de metadatos, cálculo y recálculo de sumas criptográficas en cada transferencia, trabajo exclusivo sobre copias de análisis y resguardo de una copia maestra en cadena fría; solo así debe producirse el anclaje de la huella en la red. Adicionalmente, conviene integrar controles de no manipulación (PRNU, CFA, detección de remuestreos y compresiones) y validar detectores basados en aprendizaje profundo con *benchmarks* y protocolos reproducibles para reducir falsos positivos/negativos (Reedy, 2020).

En paralelo, la calidad organizacional condiciona el valor probatorio del rastro distribuido, políticas de *forensic readiness*, roles y competencias definidos, *triage* en campo, procedimientos estandarizados, validación de herramientas, competencia del personal y revisiones por pares mitigan sesgos y errores humanos. La automatización es útil en tareas repetibles, pero la interpretación sigue siendo pericial; además, la interoperabilidad semántica (verbigracia, lenguajes comunes tipo *CASE*) facilita el intercambio entre herramientas y jurisdicciones. Operativamente, las reglas mínimas son, anclar *hashes* del original —no de impresiones ni capturas—; confrontar el *hash on-chain* con el de la imagen maestra preservada fuera de línea; auditar periódicamente consistencia, versiones de herramientas y trazas de acceso; y documentar decisiones técnicas para una valoración judicial transparente sobre autenticidad e integridad.

Continuando con el análisis pertinente, es preciso traer a colación que hasta hoy la doctrina concentra su atención en cinco exigencias funcionales sobre esta temática, proveniencia de datos, control de accesos, autenticidad/integridad, auditabilidad y privacidad/confidencialidad; por lo que se observa un déficit de marcos específicos para evidencia física y una transición incompleta de modelos a prototipos, muchos autores describen arquitecturas o marcos y pocos llegan a implementaciones verificables, lo que obliga a planificar validaciones empíricas antes del despliegue en entornos probatorios. Finalmente, es posible advertir desafíos previos al registro en cadena, tal como la fiabilidad del dato antes del anclaje, mapeo detallado del proceso de custodia y definición de una arquitectura funcional capaz de responder a los requisitos identificados. (Batista et al., 2023).

Trasladado a un plan de integración del *blockchain* a la cadena de custodia, el diseño debe comenzar por modelar el proceso de custodia (actores, eventos y evidencias) y alinear la elección de modelo de red y plataforma con los cinco requisitos señalados por la mayoría de la literatura. En términos prácticos, se empieza por optar una red permisionada cuando la visibilidad de datos y el cumplimiento normativo requieran segmentación, o por arquitecturas híbridas si se busca verificabilidad pública de huellas con resguardo privado de metadatos; seguidamente, implementar gobernanza de acceso con identidad fuerte por rol y trazabilidad auditable de cada operación; luego,

diseñar el esquema de registro priorizando proveniencia (quién, qué, cuándo y en relación con qué estado previo) y no repudio; y para finalizar, prever ensayos de prototipo que midan desempeño, costo operativo y resiliencia, conscientes de que el estado del arte muestra escasez de pruebas de concepto maduras y de referencias consolidadas para evidencia física. En suma, este análisis ofrece un conjunto de criterios de diseño verificables y alerta sobre brechas metodológicas que deben cerrarse —mapeo de procesos, garantías de dato previo al anclaje y validación operativa— para una adopción responsable. (Batista et al., 2023).

Como señalan Casino et al. (2022), la utilidad de *blockchain* en espacios probatorios depende de su inserción en un flujo forense previamente armonizado, los mayores riesgos no se encuentran en el registro distribuido, sino en las fases de adquisición y preprocesamiento, donde la heterogeneidad de fuentes, la fragmentación de datos y las contramedidas antiforenses erosionan la fiabilidad; a ello se suma la fragilidad recurrente de la cadena de custodia por fallos humanos y lagunas procedimentales, y la necesidad de reportes legibles y estandarizados que permitan reconstruir el itinerario técnico con transparencia. Desde esta perspectiva, la decisión tecnológica debe venir después del mapeo extremo a extremo de actores, evidencias, herramientas y contextos de intervención, de modo que la capa de sellado e inmutabilidad se apoye en un expediente ya validado metodológicamente.

El mismo metarrecorrido destaca que la interoperabilidad semántica y la convergencia con estándares de preservación y reporte resultan condiciones de posibilidad para cualquier despliegue con valor pericial sin un lenguaje común —por ejemplo, ontologías tipo *CASE*— y sin alineamiento con marcos como ETSI, NIST o la familia ISO 2704x, los asientos *on-chain* quedan desconectados de un expediente reproducible y comprensible para el juzgador. Casino et al. (2022) advierten, además, que ciertos artefactos críticos —telemetría de la red P2P, logs de nodos, correlaciones de IP con proveedores— quedan fuera del libro mayor y requieren gobernanza específica, al tiempo que el diseño debe tratar de origen las tensiones de jurisdicción y privacidad mediante minimización de datos en cadena y controles robustos *off-chain*. La conclusión es programática, *blockchain* añade valor como capa de sellado y trazabilidad únicamente cuando se integra en un ecosistema forense con procesos mapeados, estándares operativos y validaciones empíricas que prueben su rendimiento y reproducibilidad.

Según Patil et al. (2024), el aporte de *blockchain* a la cadena de custodia es sustancialmente procedimental, la red distribuida debe operar como parte interesada que registra, con sellado temporal y verificación interinstitucional, cada hito del ciclo probatorio sin convertirse en depósito del contenido de la evidencia. El valor emerge cuando el libro mayor refleja, de forma auditable, quién intervino, qué se transfirió, en qué momento y en continuidad con el eslabón previo. La doctrina examina arquitecturas en capas —como *Block-DEF*— y diarios de custodia en redes permisionadas con firmas múltiples, además de esquemas que refuerzan la inmutabilidad anclando periódicamente huellas en una cadena pública. En sede judicial, la consulta verificable por acusación, defensa y juzgado reduce la dependencia de declaraciones de parte y permite contrastar integridad y autoría sobre una base técnica común.

Para trasladar esa idea a una implementación responsable, el contenido probatorio permanece fuera de la cadena y solo se inscriben huellas criptográficas y metadatos mínimos, con identidades gestionadas mediante una infraestructura de clave pública por roles y con políticas de mínimos privilegios. La integración con dispositivos físicos —por ejemplo, cerraduras inteligentes cuyos estados se firman y encadenan— amplía la trazabilidad al plano material, mientras que líneas de tiempo globales y métricas de confianza forense contextualizan el peso del registro más allá del simple *hash*. Gobernanza de claves privadas, costes de infraestructura y rendimiento, es lo que exige custodia robusta de claves con módulos de seguridad hardware, segregación de funciones, rotación y revocación, además de pruebas de carga y auditorías periódicas del *ledger* y de los sistemas adyacentes. Integrada con estas cautelas, la tecnología distribuye la confianza, ofrece prueba de existencia y no alteración en fecha cierta y aporta un rastro auditable extremo a extremo que robustece, sin sustituirlas, las garantías procesales de la cadena de custodia (Patil et al., 2024).

Como sostienen Akinbi et al., (2022), la integración de *blockchain* en entornos con dispositivos conectados resulta útil cuando actúa como capa de sellado y registro verificable que endurece el itinerario probatorio frente a la volatilidad de los datos, las rutas de tránsito distribuidas y la diversidad de protocolos. Bajo ese enfoque, el contenido probatorio permanece fuera de la cadena y el libro mayor registra únicamente huellas criptográficas y metadatos indispensables, lo que permite una trazabilidad auditable entre fuentes remotas y múltiples custodios sin comprometer la confidencialidad. Las implementaciones analizadas revelan una preferencia pragmática por redes permisionadas o configuraciones híbridas con anclajes periódicos en cadenas públicas, e incluso por arquitecturas multired cuando se busca equilibrar rendimiento, coste y verificabilidad externa.

En la misma línea, la adopción responsable exige evaluar la seguridad de la infraestructura más allá de la inmutabilidad transaccional, atendiendo a riesgos de disponibilidad y a vulnerabilidades de identidad propias de sistemas distribuidos. La elección de mecanismo de consenso y su configuración condiciona la latencia y la escalabilidad, por lo que debe justificarse con mediciones reproducibles mediante *benchmarks* reconocidos, junto con métricas de consumo y coste por evento; solo con evidencia empírica y gobernanza clara —incluida la gestión de claves, el control de accesos y la conservación *off-chain*— el *ledger* puede orquestar proveniencia, integridad y rendición de cuentas a lo largo del ciclo de vida de la evidencia (Akinbi et al., 2022).

En conclusión, la adopción de *blockchain* como soporte de la cadena de custodia ofrece un refuerzo real de integridad, trazabilidad y auditabilidad, pero solo cuando se inserta en un flujo forense ya validado y compatible con los límites legales. La evidencia comparada muestra un campo en expansión que avanza a buen ritmo, aunque con carencias de implementación y evaluación empírica; la descentralización protege contra la manipulación y habilita verificación independiente, al tiempo que complica la atribución por la pseudonimidad de las direcciones y por la naturaleza transfronteriza de las redes. La inmutabilidad que preserva la prueba frente a alteraciones impide corregir *ex post* registros fraudulentos, lo que exige asegurar la licitud y la autenticidad antes del anclaje y articular mecanismos de análisis que correlacionen datos *on-chain* con fuentes *off-chain*. La complejidad de los protocolos, la aparición de criptoactivos con capas de privacidad y la necesidad de herramientas especializadas confirman que *blockchain* no sustituye el trabajo pericial ni la metodología forense, sino que la complementa con un registro resistente a la manipulación y verificable por terceros (Atlam et al., 2024).

Desde una perspectiva operativa, la integración responsable demanda gobernanza clara, estandarización y pruebas reproducibles. Los respaldos a nivel de nodo y la redundancia del libro mayor fortalecen la resiliencia y facilitan la detección de manipulaciones, pero introducen desafíos de sincronización, seguridad y control de acceso que deben resolverse en la arquitectura y en los procedimientos. La recomendación final es probar *blockchain* como una línea de tiempo probatoria que fija huellas y metadatos indispensables con fecha cierta, mantener el contenido fuera de la cadena bajo custodia pericial, y cerrar el circuito con validaciones técnicas y jurídicas que permitan al juzgador ponderar autenticidad e integridad con transparencia. Así, el marco propuesto alinea las ventajas de la inmutabilidad con las exigencias del debido proceso y con las mejores prácticas de la investigación digital. (Atlam et al., 2024).

Teniendo en cuenta lo comentado hasta este momento puede traerse a colación un caso típico para ilustrar la implementación del *blockchain* en la cadena de custodia a partir de la prueba digital. En una investigación por estafa, se incauta un teléfono y se aísla en bolsa. En laboratorio, se realiza la adquisición *bit* a *bit*, se calcula el SHA-256 de la imagen forense maestra y el dispositivo queda en cadena fría. Acto seguido, se registra en una red permisionada un asiento del contrato RegistroCustodia con el identificador del equipo, la huella de la imagen, la marca temporal, la identidad digital del perito y el enlace al último eslabón; el contenido probatorio permanece *off-chain*.

Para extraer la prueba digital (chats, SMS, bases de datos de mensajería), se trabaja solo sobre copias de análisis. Cada exportación relevante se *hashea* y se vincula *on-chain* con la imagen maestra. Cualquier traslado de custodia queda firmado y encadenado, y, de forma periódica, se

ancla un *Merkle root* en una cadena pública para prueba de existencia en fecha cierta. En juicio, el tribunal recalcula el *hash* de la imagen maestra, verifica su correspondencia con el asiento y solicita la prueba de pertenencia; si todo concuerda, queda acreditada la identidad, integridad y continuidad de los mensajes, con un rastro auditable que complementa la pericia.

IV. CONCLUSIONES

La investigación confirma que la cadena de custodia digital requiere un andamiaje técnico y jurídico más exigente que el aplicado a evidencias físicas. La preservación de identidad, integridad y autenticidad depende de adquisición *bit a bit*, resguardo de metadatos, control estricto de accesos y verificación de integridad con funciones de resumen y sellos de tiempo. El análisis–síntesis del corpus seleccionado demuestra que *blockchain* no crea por sí sola fiabilidad probatoria, pero sí ofrece una línea de tiempo distribuida que fija huellas y metadatos con fecha cierta y facilita verificación independiente por terceros.

El marco propuesto sitúa a *blockchain* como capa complementaria. El contenido probatorio permanece fuera de la cadena bajo custodia pericial; el libro mayor registra únicamente huellas y datos mínimos con trazabilidad del eslabón previo. La arquitectura recomendada privilegia redes permisionadas o diseños híbridos con anclajes públicos, gobernanza de claves mediante PKI por roles, políticas de mínimo privilegio, interoperabilidad con estándares forenses y auditorías periódicas. Bajo estas condiciones, la solución eleva la auditabilidad y reduce el espacio para disputas sobre continuidad o alteración, sin desplazar la valoración judicial ni la pericia.

Se identifica límites y retos pendientes. Existe escasez de implementaciones validadas en escenarios reales y carencias en la estandarización de reportes y semántica común. La atribución de autoría, la protección de datos personales y la coordinación transfronteriza exigen reglas claras y controles *off-chain*. Futuros trabajos deberán someter prototipos a mediciones reproducibles de rendimiento y costo, ampliar casos con evidencia física vinculada a registros distribuidos e integrar métricas de confianza forense que permitan al juzgador ponderaciones más precisas. En suma, *blockchain* resulta útil cuando se inserta en un flujo forense previamente validado y aporta valor como instrumento de trazabilidad y prueba de existencia, no como sustituto de las garantías procesales.

V. BIBLIOGRAFÍA

Akinbi, A., MacDermott, Á., & Ismael, A. M. (2022). A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models. *Forensic Science International: Digital Investigation, 42–43*, 301470. https://doi.org/10.1016/j.fsidi.2022.301470

Arellano, L., & Castañeda, C. (2012). La cadena de custodia informáticoforense. *Revista Activa, 3*,6781. https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/45/42

Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. *Electronics, 13*,3568. https://doi.org/10.3390/electronics13173568

Baracaldo-Lozano, N. A., & Daza-Giraldo, L. E. (2015). Panorama de los currículos de programas de contaduría pública en Colombia frente a contenidos de auditoría forense y prevención de delitos financieros. *Cuadernos de Contabilidad, 16*(42), 733-759. https://doi.org/10.11144/Javeriana.cc16-42.pcpc

Batista, D., Mangeth, A. L., Frajhof, I., Alves, P. H., Nasser, R., Robichez, G., Silva, G. M., & de Miranda, F. P. (2023). Exploring blockchain technology for chain of custody control in physical evidence: A systematic literature review. *Journal of Risk and Financial Management, 16*(8), 360. https://doi.org/10.3390/jrfm16080360

Bujosa Vadell, L. M., Bustamante Rúa, M. M., & Toro Garzón, L. O. (2021). La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia. *Revista Brasileira De Direito Processual Penal*, *7*(2), 1347. https://doi.org/10.22197/rbdpp.v7i2.482

Busso, M. L. (2024). Nuevo paradigma frente a la prueba digital y electrónica en el proceso judicial. *Anuario de Derecho Civil, 14*, 92–109. https://doi.org/10.22529/adc.2024(14)05

Calderón Marenco, E. A., Rodríguez Palacios, T. del S., Garzón Solano, J. E., & Ravelo-Franco, G. (2024). Construyendo la delimitación de la Lex Criptográfica. *Revista Jurídica Austral, 5*(1), 551–575. https://doi.org/10.26422/RJA.2024.0501.cal

Calderón Marenco, E. A., Garzón Solano, J. E., Sánchez Silveyra, R. M., Sal, G. O., & Ravelo-Franco, G. (2025). Responsabilidad civil del oráculo: Intersección entre el derecho privado y los contratos inteligentes. *IDP. Revista de Internet, Derecho y Política, 42,* 1-12. https://doi.org/10.7238/idp.v0i42.43070

Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Böröcz, I., Solanas, A., Conti, M., & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access, 10*, 25464–25490. https://doi.org/10.1109/ACCESS.2022.3154059

Contreras Calderón, C. A. (2021). Buenas prácticas en informática forense para el procesamiento de evidencia digital o información electrónicamente almacén. *Publicaciones E Investigación*, *15*(2). https://doi.org/10.22490/25394088.5245

Criado Enguix, J. (2025). Blockchain como medio de prueba electrónico en el marco de un proceso penal transfronterizo frente al ciberdelito. *Revista de Estudios Europeos, 85*, 492–527. https://doi.org/10.24197/ree.85.2025.492-527

Cruz Vela, E. M. (2014). Modelo para el Análisis y Gestión de Riesgos en Fases carentes de Técnicas y Herramientas: Caso Tratamiento de la Evidencia Digital en el Entorno del software libre utilizando procesos unificados. *Revista PGI*, (1), 48-56. http://revistasbolivianas.umsa.bo/pdf/rpgi/n1/n1_a10.pdf

González Granda, P., & Ariza Colmenarejo, M. J. (2021). Prueba digital y derechos fundamentales. En P. González Granda & M. J. Ariza Colmenarejo (Eds.), *Justicia y proceso. Una revisión procesal contemporánea bajo el prisma constitucional* (pp. 465-490). Dykinson. https://www.jstor.org/stable/j.ctv282jjhf.21

González, D., García, R., Barrera, A., Benítez, . L., y Acosta Adames, A. D. (2021). Reflexiones sobre manejo adecuado de cadena de custodia en nuevo proceso penal. *Revista Semilla Científica*, (2), 451–457. https://revistas.umecit.edu.pa/index.php/sc/article/view/1062

Guevara Hernández, G. A., & Mora Romero, M. L. (2025). El mal manejo de la cadena de custodia y su afectación en la investigación de la escena de un delito. *Perspectivas Sociales y Administrativas, 3*(2), 16–32. https://doi.org/10.61347/psa.v3i2.90

Jamardo Lorenzo, A. (2024). La configuración de la cadena de custodia tecnológica en el ordenamiento jurídico español. *IUS et Scientia, 10*(2), 101–122. https://doi.org/10.12795/IESTSCIENTIA.2024.i02.05

Jamardo Lorenzo, A. (2025). La dimensión tecnológica de la cadena de custodia: algunas claves. *InDret,* (2), 298–343. https://doi.org/10.31009/InDret.2025.i2.07

López Jiménez, R. (2021). La prueba en la comisión de los delitos contra la intimidad, libertad e indemnidad sexual a través de las nuevas tecnologías. En R. López Jiménez (Ed.), *Victimización sexual y nuevas tecnologías: desafíos probatorios* (pp. 61-232). Dykinson. https://www.jstor.org/stable/j.ctv2gz3wnj.6

Monti, A., & Martínez, R. (2023). Software para recolección de evidencias digitales rápidas en sistemas Windows. *Revista de Investigación en Tecnologías de la Información*, *11*(24), 103-118. https://doi.org/10.36825/RITI.11.24.009

Ochoa Arévalo, P. A. (2018). El tratamiento de la evidencia digital: Una guía para su adquisición y/o recopilación. *Revista Economía y Política,* (28), 35-43. https://doi.org/10.25097/rep.n28.2018.03

Ochoa, A. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. *Revista Economía y Política*, (28), 35-49. https://doi.org/10.25097/rep.n28.2018.03

Ovelar, S. N. (2024). Regulación expresa de la cadena de custodia en el ordenamiento jurídico paraguayo. *Revista Jurídica: Investigación en Ciencias Jurídicas y Sociales, 14*(2), 77–94. https://dialnet.unirioja.es/servlet/articulo?codigo=9706862

Patil, H., Kaur Kohli, R., Puri, S., & Puri, P. (2024). Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework. *Egyptian Journal of Forensic Sciences, 14*(12). https://doi.org/10.1186/s41935-023-00383-w

Reedy, P. (2020). Interpol review of digital evidence 2016–2019. *Forensic Science International: Synergy, 2*, 489–520. https://doi.org/10.1016/j.fsisyn.2020.01.015

Sánchez Prada, M. D. & Mora Izquierdo, R. (2001). Investigación forense del "Asalto sexual". *Revista de la Facultad de Medicina*, *49*(3), 169–174. https://revistas.unal.edu.co/index.php/revfacmed/article/view/19784

Vacaro Bolívar, F. del C. (2025). Las evidencias y elementos de interés criminalística colectadas en la escena del crimen. *Revista Arbitrada Orinoco Pensamiento y Praxis, 15*(1), 43–58. https://revistaorinocopyp.org.ve/index.php/home/article/view/44