# La *blockchain* como tecnología aplicable a la cadena de custodia ¿Puede esta tecnología mejorar el resguardo de la evidencia?

José G. Damiani Corraro, Lara M. Quevedo Arcuri e Iván E. Sarapura

Facultad de Derecho, Universidad de Buenos Aires

LegalThon - Hackathon Académico de Gobernanza Descentralizada

Sofía M. Barros Mendez

24 de noviembre de 2025

**Resumen**

La cadena de custodia de la evidencia digital representa una vulnerabilidad crítica en el sistema judicial moderno. En este sentido, la naturaleza volátil, intangible y fácilmente alterable de la evidencia digital genera una incertidumbre procesal que amenaza el debido proceso, como lo demuestran antecedentes jurisprudenciales argentinos (ej. Casos "Vélez Cheratto" de la Cámara Federal de Casación Penal y "Ricardo Jaime" de la Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal). Estos han demostrado de manera inequívoca que la falta de protocolos técnicos robustos ha puesto en riesgo o ha resultado en la nulidad de pruebas clave.

La presente investigación postula que la tecnología *blockchain*, gracias a sus características de inmutabilidad, trazabilidad criptográfica y descentralización, ofrece una solución técnica robusta para sellar la integridad de la evidencia digital. A través de un análisis del estado del arte, se estudia la problemática técnica y el marco legal. Además, se examina el derecho comparado, incluyendo casos pioneros en los Tribunales de Internet de China (ej. Hangzhou Huatai) y la legislación específica de Estados Unidos (Illinois Blockchain Technology Act). Posteriormente, se analiza el contexto argentino, revisando su base doctrinal y el primer antecedente jurisprudencial sobre la Blockchain Federal Argentina (ej. Fallo R.S.G.D.J. c./B.A.V. de la Cámara de Apelación en lo Civil y Comercial del Departamento Judicial de Morón).

Finalmente, se presenta una propuesta de implementación concreta para Argentina, la cual no buscará reemplazar la cadena de custodia tradicional, sino complementarla, sugiriendo un anteproyecto de ley que utilice la infraestructura existente de Cardano para el registro inmutable de los *hashes*. Este modelo mantendrá el contenido sensible *off-chain,* lo que garantizará tanto la integridad pública de la evidencia como la confidencialidad del expediente.

## 1. Introducción

El derecho enfrenta el desafío constante de adaptar sus estructuras a una realidad en perpetua transformación; ningún sistema puede mantenerse estático sin incorporar los nuevos avances en su propio funcionamiento. El problema radica en que, actualmente, la velocidad de la innovación tecnológica ha superado la capacidad de asimilación de muchos ordenamientos, situación que genera normativas anacrónicas que desconocen cómo solucionar los desafíos que surgen en la era digital. Sin embargo, durante la última década, numerosos sistemas normativos alrededor del mundo han empezado a considerar la *blockchain* y sus elementos derivados como piezas clave para sus ordenamientos jurídicos.

Adicionalmente, debido al paulatino auge en el interés de estas tecnologías, se ha democratizado el acceso a la información y cada vez se cuenta con más desarrollos íntegros sobre su funcionamiento. Esta coyuntura lleva a que, inexorablemente, se deba considerar en cada ordenamiento y a través de normas específicas, cómo se encuadran estos nuevos sistemas dentro de los hechos y actos jurídicos de la vida real.

Estamos, entonces, ante una oportunidad única de proponer nuevas formas de entender el derecho a través de la *blockchain*. El interrogante central ha dejado de ser la viabilidad de la aplicación de la blockchain, para centrarse en la metodología correcta de su implementación. En ese marco, el presente estudio se propone analizar y estudiar casos reales de su aplicación, para finalmente proponer una forma de darle uso en el ordenamiento argentino, específicamente en su aplicación a la cadena de custodia de la evidencia.

A estos fines, resulta crucial aclarar el enfoque: la *blockchain* no se abordará como un medio de prueba en sí, sino como una herramienta de resguardo y certificación para garantizar la integridad y existencia de la evidencia digital en un momento determinado.

A tal efecto, el desarrollo del trabajo se realizará de manera armónica y ordenada. En primer lugar, se definirá el concepto de *blockchain* y sus tecnologías relacionadas, para entender el estado de situación actual. En segundo lugar, se analizará la cadena de custodia de la evidencia y los inconvenientes que podrían ser solucionados por la *blockchain*. En tercer lugar, se examinará la utilización de esta tecnología en casos de otros ordenamientos normativos internacionales. En cuarto lugar, se abordará en profundidad el objeto central de este análisis, esto es si pueden las nuevas tecnologías facilitar el resguardo de la evidencia digital. Finalmente, se propondrá un mecanismo para introducir la *blockchain* al resguardo de evidencia en el sistema jurídico argentino. De esta manera, se obtendrá una aproximación efectiva y necesaria de cómo la *blockchain* puede contribuir a mejorar la justicia argentina.

## 2. Fundamentos técnicos: Idoneidad de Cardano para la custodia digital

La tecnología *blockchain* ofrece un registro distribuido e inmutable donde las transacciones se validan por una red de nodos y se sellan criptográficamente. Esta arquitectura genera una mayor confianza debido a su naturaleza descentralizada, siendo ideal para la cadena de custodia.

Para aplicar esta arquitectura a la custodia digital, dos conceptos técnicos son centrales. Primero, debe entenderse que el *hashing* es una operación criptográfica que transforma cualquier dato (ej. un documento o una pericia) en una "huella digital" alfanumérica, única e irrepetible (Narayanan et al., 2016). Esta huella garantiza la integridad del dato: si el archivo original se altera en lo más mínimo, su *hash* cambia por completo. En segundo lugar, debe tenerse presente que la *tokenización* es el proceso de tomar esa "huella digital" (el *hash*) y convertirla en un activo digital único (Voshmgir, 2020) que puede ser registrado y transferido dentro de la *blockchain*. Esto permite crear un "gemelo digital" de la evidencia (usualmente como un NFT - *Non Fungible Token*), garantizando su trazabilidad inequívoca.

Con estos conceptos en mente, para un caso de uso de alta sensibilidad como lo es el sistema judicial, se requiere una red que combine seguridad, sostenibilidad y un sistema de gobernanza claro. Por ello, se propone el ecosistema Cardano por sus características técnicas diseñadas con un enfoque metodológico probado. A diferencia de las redes de primera generación, Cardano ofrece una arquitectura de capas, la cual separa la liquidación del cómputo (Hoskinson, 2017). Esto es ideal para aplicaciones de alta carga, puesto que ofrece la flexibilidad de procesar la lógica de la aplicación sin congestionar la capa principal de consenso de la red. En suma, Cardano otorga seguridad y sostenibilidad (a través de Ouroboros). Esto se debe a que su protocolo *Proof-of-Stake* (PoS) está formalmente verificado, ofreciendo una seguridad robusta con un consumo energético mínimo, lo cual constituye un factor clave para la adopción institucional a largo plazo (Kiayias et al., 2019). Pero además, su sistema de gobernanza descentralizada (Voltaire) permite que la red evolucione de forma transparente, siendo este un modelo opuesto a las redes permisionadas (como la Blockchain Federal Argentina) donde la confianza recae en un consorcio cerrado.

## 3. Vulnerabilidades críticas en la cadena de custodia tradicional

En este punto, es necesario definir a la cadena de custodia de la prueba, al menos en el sistema argentino. El manual del Ministerio Público Fiscal define a esta cadena como *"el conjunto de medidas que deben adoptarse a fin de preservar la identidad e integridad de*

*objetos o muestras que pueden ser fuente de prueba de hechos criminales, para su total eficacia procesal" (MPF, 2015, p. 1).*

Aunque esta definición del Ministerio Público Fiscal se enmarca en el proceso penal, la problemática se ha vuelto universal. En la era digital, la validez de un correo electrónico en un juicio laboral, un contrato digital en un litigio comercial o una captura de pantalla en un caso de familia, enfrenta los mismos desafíos de integridad y autenticidad. Por lo tanto, las vulnerabilidades aquí descritas son comunes a toda la prueba digital del ordenamiento.

El inconveniente con este sistema tradicional de la cadena de custodia, que fue diseñado principalmente para la evidencia física, es que muestra profundas insuficiencias en la era digital. La propia necesidad de crear protocolos específicos por parte de organismos como el Ministerio Público Fiscal (MPF) evidencia que los métodos tradicionales son inadecuados. Estos nuevos protocolos reconocen que el manejo de la prueba digital exige "técnicas científicas y analíticas especializadas" y la intervención de "personal especialista", superando la capacidad del mero "primer interviniente" (MPF, 2023, p. 2). Informes del instituto de Estudios Comparados en Ciencias Penales y Sociales (INECIP) confirman que el paradigma digital trajo enormes problemas y expuso serias deficiencias en la capacitación de los operadores, lo cual puede comprometer la válida introducción al proceso de la evidencia (Corti, 2025).

Esta insuficiencia se agrava por la naturaleza misma de la prueba digital, definida por la doctrina como "volátil" y de "fácil adulteración". Autores como Piottante y Agüero la han descrito con precisión como *"sensibles, de fácil cambio de estado, de posible manipulación y difícil validez probatoria"* (Agüero y Piottante, 2023, p. 2). Esta fragilidad genera una incertidumbre constante en los procesos judiciales. Consecuentemente, la carga de la validación se traslada a los litigantes, quienes deben recurrir a costosas pericias para intentar acreditar la integridad de pruebas que son pilares de sus casos. Finalmente, el riesgo de ser desestimadas es tangible: la doctrina es clara al advertir que una ruptura en la cadena de custodia, un riesgo latente desde la recolección inicial, puede acarrear la exclusión de la prueba por causa de nulidad (Gaiardo, 2018).

Esta fragilidad inherente, a su vez, choca directamente con los principios forenses internacionalmente aceptados, como los de la norma ISO 27037 (Lavin y Llanos, 2024). Esta exige que el manejo de la evidencia digital, refiriéndose a su identificación, recolección, adquisición y preservación, cumpla con principios estrictos de "Auditabilidad, Justificabilidad, Repetibilidad y Reproducibilidad" (Lavin y Llanos, 2024, p. 3). Son

precisamente estos requisitos los que los métodos tradicionales de actas en papel y la simple firma de un funcionario no pueden garantizar por sí solos en el volátil entorno digital.

**4. Antecedentes jurisprudenciales: Fallas en la custodia de la evidencia**

Un ejemplo paradigmático de esta problemática en Argentina es el fallo Vélez Cheratto, Emanuel s/recurso de casación del año 2018. Este caso se originó a raíz de un ciberataque en el que la defensa solicitó la nulidad de toda la evidencia digital, incluyendo capturas de pantalla y copias almacenadas en pendrives, alegando que el personal policial no utilizó un bloqueador de textos ni realizó el cálculo del *hash* de la copia forense, incumpliendo los protocolos estándar de recolección. Pese a que la Cámara Federal de Casación Penal finalmente rechazó la nulidad, no lo hizo porque la prueba fuera técnicamente intachable, sino porque los peritos actuaron en concordancia con los protocolos, a pesar de la omisión. Las copias fueron certificadas por personal idóneo y, fundamentalmente, dos fiscales estuvieron presentes durante el procedimiento.

Si bien se salvó la evidencia, esto demuestra que la validez de la prueba digital en Argentina hoy depende de factores externos, como la presencia de un fiscal o el testimonio de peritos, y no de una garantía técnica e inmutable de su integridad. Ante esta situación cabe preguntarse cuál habría sido el desenlace ante la ausencia de los fiscales. La tecnología *blockchain* tiene la capacidad de eliminar esta incertidumbre.

Un antecedente aún más emblemático de esta vulnerabilidad es el conocido caso “Ricardo Jaime”, donde la Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal declaró la nulidad de un peritaje clave sobre las computadoras secuestradas. El problema central fue una ruptura flagrante de la cadena de custodia.

Un segundo peritaje, realizado por la Universidad de Buenos Aires (UBA), y un tercero, por la Universidad Tecnológica Nacional (UTN), constataron que el material no había sido debidamente resguardado. El informe de la UTN fue categórico al aseverar que se detectaron numerosos archivos que fueron creados o modificados después del secuestro, mientras estaban bajo custodia policial. Los peritos destacaron explícitamente la falta de uso de bloqueadores de escritura, lo que llevó a la “contaminación” de la evidencia, concluyendo así la Cámara que las prácticas policiales habían comprometido irremediablemente la evidencia. Este caso es un ejemplo representativo de cómo la falla en los protocolos, como la falta del cálculo de *hash* y bloqueadores, no constituyen un mero formalismo, sino una omisión que puede destruir materialmente el valor probatorio de la evidencia digital.

## 5. Derecho comparado: Experiencias internacionales en la aplicación de la *blockchain*

Dado que esta investigación se centra en determinar la aplicabilidad de la *blockchain* en el ordenamiento argentino, donde se carece de un cuerpo legislativo o jurisprudencial sólido y consolidado sobre la materia, resulta académicamente indispensable analizar la experiencia en otras jurisdicciones. Este análisis de derecho comparado permite estudiar los pasos dados por sistemas pioneros, ya sea por vía legislativa (ej. Illinois, EE.UU.) o por adopción judicial temprana (ej. China y España). El objetivo es identificar soluciones exitosas y evitar escollos ya transitados, para así construir una propuesta superadora.

En el sector privado, *"la falta de leyes claras y uniformes sobre blockchain y criptomonedas genera dudas para empresas e inversores"* (Artica, 2024, párr. 10), lo cual también genera cierta reticencia en su aplicación y una mayor confianza en antiguos sistemas que, aunque no sean tan seguros como la *blockchain*, se encuentran regulados y estudiados por las legislaciones locales. Por otro lado, en el sector público y los sistemas judiciales tampoco hay regulaciones específicas sobre este sistema, y esto lleva a que se generen lagunas legales o problemas de aplicación de las normas positivas a casos que involucren *blockchain*. Esta situación reviste especial gravedad si tomamos en consideración que, en muchas ocasiones, se intenta adaptar normas sobre otros ámbitos para decidir sobre casos que involucren a esta tecnología, lo cual deriva en una mala interpretación o un deficiente entendimiento de cómo funciona, lo cual genera más incertidumbre. No obstante, existen antecedentes aislados donde se ha logrado una armonización técnica y jurídica exitosa en sistemas legales preexistentes. En consecuencia, el examen pormenorizado de estas experiencias comparadas resulta indispensable para dilucidar un camino de implementación viable.

### 5.1. China: La adopción judicial y el precedente de Hangzhou

En primer lugar, la República Popular China ha sido pionera en la adopción judicial de esta tecnología. El caso fundacional es *Hangzhou Huatai Culture Media Co., Ltd. v. Shenzhen Daotong Technology Development Co., Ltd.* (2018), tramitado ante el Tribunal de Internet de Hangzhou. En este litigio sobre infracción de derechos de autor, el demandante presentó como prueba capturas de pantalla de la página web infractora. Para probar su autenticidad utilizó un servicio de terceros llamado Baoquan.com que capturó la página web y su código fuente, calculó el valor *hash* SHA256 de esta evidencia, y subió dicho *hash* a las *blockchains* públicas de Bitcoin y Factom (Zou y Chen, 2024).

El Tribunal de Internet de Hangzhou realizó un análisis técnico de tres pasos. Verificó la neutralidad de la plataforma de preservación de la prueba, confirmó la fiabilidad de los medios técnicos de captura y dio fe de la integridad de la preservación en *blockchain*. Es decir que el propio tribunal verificó que el *hash* del archivo descargado coincidía con el *hash* almacenado en las *blockchains* públicas. Así, el Tribunal concluyó que este método aseguraba efectivamente la integridad de los datos y, por lo tanto, aceptó la evidencia respaldada por la *blockchain* como prueba válida de la infracción.

Este fallo a su vez fue ratificado por la Corte Suprema Popular de China, que reconoció que las cortes de internet pueden aceptar evidencia autenticada por *blockchain*. A la vez, es preciso señalar que en la actualidad China opera con múltiples *blockchains* judiciales oficiales, las cuales a menudo colaboran con gigantes tecnológicos como Alibaba y Baidu (Wang, 2021, p. 4).

### 5.2. Estados Unidos: El reconocimiento legislativo de Illinois

Por otro lado, en Estados Unidos, en lugar de esperar a la jurisprudencia, algunos estados han optado por recurrir a la vía legislativa. El caso más notable es la *Blockchain Technology Act* del estado de Illinois (Illinois General Assembly, 2020).

Esta ley otorga reconocimiento legal directo a la tecnología *blockchain*; su sección 10(b) establece inequívocamente que *"En un procedimiento, la evidencia de un contrato inteligente, registro o firma no debe ser excluida únicamente porque se utilizó una blockchain para crear, almacenar o verificar dicho contrato inteligente, registro o firma"* (traducción propia; Illinois General Assembly, 2020). Además, la ley aclara que si una norma requiere un registro "por escrito" o una "firma", un registro o firma contenida en la *blockchain* satisface dicho requisito. Sin embargo, la ley también establece limitaciones importantes, como la prohibición de usar *blockchain* para notificaciones de desalojo, ejecuciones hipotecarias o cancelación de seguros de salud.

### 5.3. España: Desafíos procesales ante la ausencia de regulación específica

A su vez, en España, el tratamiento procesal de la prueba digital evidencia la falta de un desarrollo normativo específico que la *blockchain* busca solucionar. Como analiza Pérez Campillo, la legislación española actual, más específicamente la Ley de Enjuiciamiento Civil (en adelante LEC), no reconoce explícitamente los registros en la *blockchain* como "documentos públicos probatorios válidos". Por lo tanto, deberían ser presentados como prueba documental privada de conformidad con el artículo 326.1 LEC. Por ello, de ser

impugnada esta prueba, se vuelve imprescindible la presentación de un informe pericial informático que verifique la autenticidad e integridad del archivo en cuestión y explique el funcionamiento de la *blockchain* al tribunal (Pérez Campillo, 2024, p. 5).

Este escenario de incertidumbre probatoria queda de manifiesto en la propia jurisprudencia española. En el caso STS 326/2019, ante la falta de una pericia técnica sobre correos electrónicos, el Tribunal Supremo tuvo que recurrir a un complejo análisis de indicios y testimonios, como las declaraciones de las víctimas y aseverar contradicciones por parte del acusado, para establecer la autenticidad de la comunicación (Tribunal Supremo de España, 2019).

Este escenario de incertidumbre probatoria es precisamente el que la tecnología *blockchain* busca resolver. A diferencia del caso analizado por el Tribunal Supremo, el uso de un sistema de preservación de evidencia basado en *blockchain*, como lo visto en la jurisprudencia china en el caso de Hangzhou y las propuestas de la *Blockchain Technology Act* de Illinois en EE.UU., proporcionan un sello de tiempo y un *hash* criptográfico antes del litigio, ofreciendo una garantía de integridad técnica que no depende netamente de la prueba testimonial.

## 6. La *blockchain* en el sistema legal argentino: Vacío normativo y precedentes

Actualmente, en Argentina no existe una legislación específica que regule el uso de la tecnología *blockchain* en la cadena de custodia. Este vacío legal genera la incertidumbre central de esta investigación: ¿cómo puede el sistema judicial valorar un registro en *blockchain* si no está contemplado en el ordenamiento jurídico?

A estos fines resulta importante aclarar que la *blockchain* no debe ser confundida con un medio de prueba en sí mismo. La evidencia es el documento electrónico, la fotografía, el video, el audio, etc. La *blockchain*, en cambio, es una herramienta tecnológica de resguardo y certificación; su función no es probar el contenido del acto (ej. si lo dicho en un contrato es verdadero o si una firma fue vulnerada), sino probar la integridad y existencia de esa evidencia digital en un momento determinado.

### 6.1. Jurisprudencia nacional: El precedente “Ruiz Solís” y la BFA

Esta distinción fundamental ya ha sido delineada por la jurisprudencia argentina. Un fallo trascendental es la sentencia de la Cámara de Apelaciones en lo Civil y Comercial de Morón en la causa “R.S.G.D.J. c/ B.A.V.” (2024). En este caso, una compañía de seguros

presentó como prueba un convenio electrónico que había sido “sellado” en la Blockchain Federal Argentina (BFA).

El tribunal, en el voto del Dr. Gallo, realizó un análisis técnico preciso y determinó que la BFA no almacena el documento, sino únicamente su *hash* (huella digital). Sin embargo, el elemento central que otorgó viabilidad a la BFA en el proceso no fue únicamente su arquitectura técnica, sino un argumento de confianza institucional que el propio tribunal invocó: la BFA es la infraestructura que el propio Estado Nacional utiliza para garantizar la fiabilidad del Boletín Oficial de la República Argentina (Boletín Oficial, 2017).

Este razonamiento es fundamental, ya que establece una suerte de doctrina de los actos propios a nivel estatal: si el Poder Ejecutivo Nacional confía en la BFA para una función de fe pública tan crítica como es el resguardo inmutable de las publicaciones del Boletín Oficial, el Poder Judicial se ve compelido a aceptar, al menos, su idoneidad técnica para una función análoga de certificación.

La conclusión del fallo fue crucial, al determinar, en primer lugar, que la *blockchain* permite certificar la existencia de un documento electrónico en un momento determinado y su inalterabilidad hasta el momento de la verificación. Es decir, prueba fehacientemente la integridad y la fecha cierta del *hash*. Pero además de ello, se determinó lo que no prueba la *blockchain*, ya que el tribunal dictaminó expresamente que el sellado, por sí solo, no asegura su cumplimiento, ni que se firmó, ni quien lo firmó, ni la exactitud de su contenido.

Por lo tanto, el fallo revocó la decisión de primera instancia y ordenó que el documento (cuya integridad fue probada por la BFA) debía ser analizado en conjunto con el resto de las pruebas para determinar si la transacción realmente había existido. En definitiva, la BFA no fue la prueba, sino el resguardo que blindó la integridad de la evidencia documental.

### 6.2. El primer *smart contract* legalmente ejecutable

Si el fallo Ruiz Solís demuestra la viabilidad de la *blockchain* (BFA) como una herramienta para el resguardo de la prueba, un hito de la práctica legal demuestra la viabilidad de la *blockchain* como herramienta de ejecución contractual. Se hace referencia al primer *smart contract* reconocido como legal y judicialmente ejecutable en Argentina.

El caso consistió en un contrato de mutuo (préstamo) por 10.000 tokens ADA (la criptomoneda nativa de Cardano), con plazo e interés, desarrollado por la startup legaltech dLab sobre la plataforma Plutus de la *blockchain* de Cardano (Harkavy, 2024). La relevancia de este acto radica en dos factores: en primer lugar, que las partes vincularon el contrato

*on-chain* con un documento legal *off-chain* que identifica a las partes y las billeteras, creando un modelo híbrido ejecutable; y en segundo lugar, que su validez se enmarca en la autonomía de la voluntad y las disposiciones del DNU 70/2023 (Presidencia de la Nación, 2023), que habilita el uso de criptomonedas en contratos.

Este precedente, si bien no se refiere a la cadena de custodia, es de vital importancia para nuestro análisis. Demuestra que la jurisdicción argentina ya está reconociendo la validez de operaciones hechas en la *blockchain*. Si dicha tecnología es considerada lo suficientemente robusta para la ejecución de obligaciones contractuales privadas, su idoneidad para una función menos compleja, como la que propone la presente investigación, se ve sustancialmente reforzada.

### 6.3. Libertad probatoria y mecanismo atípico

Si la *blockchain* es un "resguardo", ¿cómo se valora en juicio? La respuesta la da el principio de libertad probatoria, consagrado en los códigos procesales, que permite a las partes probar los hechos por cualquier medio, siempre que sea legal.

Como señala la Dra. Leticia Melo, el registro en *blockchain* debe ser considerado un elemento atípico (Melo, 2019). Esto se debe a dos razones: primero, la falta de una normativa específica que la regule en los códigos de fondo, y, segundo, porque el procedimiento de validación de la *blockchain* (descentralizada, algorítmica, sin intervención humana directa) no tiene analogía con los medios de prueba típicos (testimonial, documental, pericial).

Por lo tanto, el registro *hash* en *blockchain* debe ser valorado por el juez, mediante la sana crítica, como un elemento de convicción atípico o un mecanismo de certificación de prueba aún no regulado. Al final, su única finalidad es robustecer la trazabilidad e integridad de la evidencia principal.

### 6.4. Obligaciones internacionales y doctrina local

Al mismo tiempo, el Convenio de Budapest tiene carácter supralegal otorgado por nuestra Constitución Nacional, lo que hace que nuestras leyes deban adaptarse a la jerarquía normativa establecida en la misma. No solo eso, sino que además la Convención de Viena sobre el Derecho de los Tratados (Comisión de Derecho Internacional, 1969) establece en su artículo 27 que un Estado no podrá invocar su derecho interno como justificativo para el incumplimiento de un tratado; es decir, la falta de legislación interna no puede justificar la falta de medidas estatales que salvaguarden los datos electrónicos establecidos en el Convenio de Budapest sobre la ciberdelincuencia (ETS n.º 185; Consejo de Europa, 2001).

Por otra parte, la doctrina nacional también se ha abocado a abordar esta problemática. Ya en el año 2022, Miguel Luis Jara en su artículo "*Blockchain* y derecho. Un abordaje preliminar", concluía que *"la irrupción de las nuevas tecnologías en todos los aspectos de la vida de las personas ha causado profundas innovaciones en todos los estamentos, es por ello que el derecho, siempre fiel a su rol social, no puede mantenerse ajeno"* (Jara, 2022, sección XII, párr. 1).

Adicionalmente, en 2023 se publicó "Nuevas tecnologías: *blockchain*, cripto activos y smart contracts", escrito por el Dr. Germán Grosso Molina. En ese trabajo, el autor señala los beneficios que la *blockchain* tiene y cómo podría beneficiar los procesos judiciales en nuestro país. A través de un análisis exhaustivo, llega a una conclusión certera: "*...estas tecnologías ocasionarán situaciones que en algún momento serán motivo de consulta en estudios jurídicos, y eventualmente, objeto de reclamo judicial. Para eso, los operadores jurídicos deberemos estar capacitados y al tanto de lo que está ocurriendo"* (Grosso Molina, 2023, sección IV, párr. 5).

En este contexto, el antecedente doctrinario más relevante en la materia es el trabajo de Daniel Fernando Gaiardo "Uso de la tecnología para mejorar la cadena de custodia". Este trabajo es un antecedente directo de la propuesta aquí vertida, puesto que propone implementar en conjunto la *blockchain* y la firma digital para asegurar el proceso de la cadena de custodia de la evidencia digital. El autor concluye que la *blockchain* puede revolucionar la cadena de custodia, asegurando la transparencia, autenticidad e inmutabilidad de la prueba digital (Gaiardo, 2018).

Como punto fundamental, Gaiardo propone no reemplazar la cadena de custodia física, sino complementarla, creando una *blockchain* privada judicial donde cada evidencia quedaría registrada como una transacción validada. En sus propias palabras, *"de esta manera recorriendo toda la cadena de bloques se podría reconstruir la trazabilidad o cadena de custodia de la prueba digital"* (Gaiardo, 2018, sección IX, párr. 3).

Esta visión se alinea con la práctica del propio Estado. El Ministerio Público Fiscal, en su manual, ya reconoce la necesidad de que al recoger elementos de prueba se debe tener el cuidado suficiente de "no alterar su esencia", con el objeto de mantener su integridad tal cual fueron hallados (MPF, 2015, p. 2).

Tomando los antecedentes doctrinarios, las normas supralegales y el principio de libertad probatoria analizado, es posible trazar una conclusión precisa. Las obligaciones internacionales (Convenio de Budapest, artículo 16; Consejo de Europa, 2001) imponen al Estado el deber de implementar medidas efectivas para la "conservación" de la evidencia

digital. Paralelamente, la doctrina local (Gaiardo, 2018; Jara, 2022; Grosso Molina, 2023) ha identificado que la tecnología *blockchain* es el sistema técnico idóneo para cumplir esa función de resguardo.

Finalmente, el principio de libertad probatoria y el concepto de prueba atípica, tratado en la sección anterior, proporcionan el vehículo procesal para que el resultado de dicho sistema (el registro de *hash* inmutable) sea introducido y valorado en el sistema judicial.

## 7. Respuesta a la hipótesis: La *blockchain* como solución de resguardo

La respuesta a la hipótesis central de este estudio es afirmativa: la tecnología *blockchain* puede, y debe, ser utilizada para mejorar la cadena de custodia de la prueba. Esto se debe a su amplia fiabilidad criptográfica, demostrada en proyectos de alta seguridad como Cardano, que se presenta como un sistema idóneo al reforzar esta cualidad mediante un desarrollo fundamentado en la investigación académica y métodos formales, priorizando la seguridad de la red. De esta forma, se ofrece una solución técnica a un problema que hasta ahora dependía de la fe pública y de protocolos físicos falibles.

Sin embargo, su aplicación no debe ser arbitraria, sino que exige un marco legal y técnico preciso. Si el objetivo es garantizar la integridad y el seguimiento de las pruebas, su implementación debe ser impecable.

### 7.1. La solución: Un enfoque complementario

La propuesta de esta investigación no es sustituir la cadena de custodia actual, sino complementarla y fortalecerla. El sistema tradicional, basado en actas, sellos y la firma de funcionarios, es indispensable para la custodia física. El problema, como se demostró en los casos Ricardo Jaime y Vélez Cheratto, radica en la evidencia digital, que es intangible y fácilmente alterable.

Aquí es donde la *blockchain* ofrece una solución concreta. El principal inconveniente del sistema tradicional es que estas formas de asegurar la autenticidad se encuentran centralizadas en la figura del funcionario custodio y, por lo tanto, son susceptibles de errores humanos, omisiones protocolares o, inclusive, de manipulación a través de ataques maliciosos que tengan por fin dilatar el proceso o directamente desestimarlo. La *blockchain* soluciona esto al reemplazar la confianza centralizada en una persona por la verificación descentralizada de un sistema criptográfico.

Cualquier alteración a una prueba cuyo *hash* ya fue registrado sería detectable inmediatamente, pues la huella digital resultante no coincidiría con la registrada en la cadena

de bloques inmutable. De esta manera, el registro de la cadena de custodia deja de depender de la diligencia o el cuidado de un funcionario y pasa a estar en manos de un sistema de verificación colectiva.

### 7.2. El modelo técnico: Integridad, trazabilidad y descentralización

La implementación de este sistema es posible gracias a los fundamentos técnicos de la *blockchain*, que resuelven directamente los puntos débiles de la custodia tradicional.

El primer problema resuelto es el de la integridad (esto a través del *hashing*). Bajo este esquema, la blockchain no almacena la evidencia en sí, sino que cada evidencia digital (sea un documento, una foto o una copia forense) es pasada por una función *hash*, creando una huella digital alfanumérica única y es solo este *hash* el que se registra en la *blockchain*. Esto resuelve el problema de la "contaminación" de la prueba, visto por ejemplo en el caso Ricardo Jaime.

En segundo lugar, se resuelve la problemática de la trazabilidad a través de la tokenización**.** Cada *hash* registrado puede ser "tokenizado", creando un objeto digital único denominado NFT (*Non Fungible Token*) que represente a esa evidencia específica. Por lo tanto, cada vez que esa evidencia cambia de custodia (por ej., del perito al juzgado y del juzgado a la Cámara), se registra una nueva transacción vinculada a ese token. Esto crea un registro cronológico, transparente e inalterable de cada movimiento de la evidencia.

Por último, la descentralización garantiza que esta base de datos o "libro mayor" que contiene los *hashes* y registros de trazabilidad, no resida en una sola computadora, sino que está replicada en múltiples nodos o "servidores" distribuidos en los actores clave del sistema judicial, así eliminando el riesgo de un punto único de falla.

### 7.3. Requisitos de implementación: Legalidad, privacidad y gobernanza

La viabilidad de este sistema depende de tres consideraciones preliminares fundamentales, las cuales constituyen los pilares de la propuesta desarrollada en la sección siguiente.

En primer lugar, se requiere un marco legal claro y efectivo. Si bien la problemática es transversal a todos los fueros (penal, civil, laboral, etc.), la ley debe establecer claramente el alcance de la tecnología. Esta norma debería establecer cuáles son los medios probatorios a los cuales podrían aplicarse y aceptarse el uso de la *blockchain*. En este sentido, se propone una norma que defina qué constituye un registro en *blockchain* y, fundamentalmente, que le

otorgue presunción iuris tantum de integridad al *hash* de una evidencia registrada bajo el protocolo oficial.

Un segundo aspecto crítico es la confidencialidad y el manejo de datos personales. La tensión entre la transparencia pública de la *blockchain* y la normativa vigente sobre protección de datos personales (Ley 25.326; Congreso de la Nación, 2000) se resuelve mediante la propia arquitectura del sistema, dado que la *blockchain* nunca almacena información sensible en texto plano. La evidencia (el documento, la foto, el video, etc.) permanece "fuera de la cadena" (*off-chain*), resguardada en repositorios judiciales seguros y protegida por el secreto de sumario y las leyes de protección de datos vigentes. Lo único que se registra en la *blockchain* (*on-chain*) es el *hash* asignado a la evidencia, que se trata de una cadena de texto seudonimizada que no revela contenido alguno. De esta forma se logra la integridad pública y confidencialidad del contenido.

Finalmente, debe existir una óptima gobernanza y descentralización. El sistema debe ser confiable y para ello es de vital importancia diferenciar dos conceptos fundamentales. La descentralización, desde una perspectiva técnica, se refiere a la distribución física de los nodos. La propuesta, alineada con la del Dr. Gaiardo (2018), sugiere que los nodos validadores estén en los juzgados, Cortes Provinciales y Ministerios Públicos, eliminando el control centralizado del sistema. A su vez, desde una perspectiva de gobernanza, se refiere a las reglas de este sistema y cómo se llega a un consenso entre los participantes para, por ejemplo, decidir sobre futuras modificaciones o actualizaciones del sistema.

En conclusión, la *blockchain* puede resguardar la cadena de custodia si se utiliza como lo que es: una herramienta de certificación y trazabilidad descentralizada, auditable y sujeta a control judicial. Su implementación bajo un modelo *off-chain* y con una gobernanza robusta, garantiza, simultáneamente, la efectiva tutela de los derechos fundamentales y la confidencialidad de la información de cada prueba recolectada.

## 8. Propuesta de aplicación al sistema legal argentino

La experiencia comparada, sumado a los primeros antecedentes conceptuales en el ámbito nacional, demuestran que la adopción de la *blockchain* es viable, pero requiere de un marco normativo que le otorgue sustento y uniformidad. Basado en el análisis de la presente investigación, es posible proponer un anteproyecto que se denominará "Ley de Evidencia Digital y Blockchain" para la República Argentina. Este debería estar basado en cinco pilares fundamentales.

En primer lugar, es necesario el reconocimiento legal expreso en el propio ordenamiento jurídico. Esto implicaría incorporar en los Códigos Procesales explícitamente el valor probatorio del sellado de tiempo en *blockchain* denominado *timestamp*. Se propone añadir un artículo que establezca que el registro de un valor *hash* de un documento o archivo digital realizado mediante el protocolo técnico oficial (sidechain o *Layer 2* judicial) gozará de una presunción *iuris tantum* de integridad y fecha cierta desde el momento de su registro, siempre que su anclaje a la *Layer 1* pública de confianza sea verificable.

En segundo lugar, se requerirá la adopción de la *blockchain* de Cardano. Si bien la Blockchain Federal Argentina (BFA) representa un primer paso valioso, su naturaleza de red permisionada (federada) replica un modelo de confianza centralizado. Por lo tanto, para una implementación en el sistema judicial, que demanda la máxima transparencia, neutralidad y seguridad, se propone utilizar la arquitectura de la *blockchain* de Cardano como principal capa de confianza para la cadena de custodia de la prueba digital.

En tercer lugar, será indispensable implementar una *Sidechain* o *Layer 2* para la infraestructura judicial: La operatoria diaria (el registro de miles de *hashes* de evidencia por parte de peritos y funcionarios) se realizaría en una *Layer 2* permisionada, optimizada mediante soluciones de escalabilidad nativas como Hydra, en la cual los nodos serían operados por los actores del sistema de justicia (Cortes Provinciales, Ministerios Públicos), de forma similar a la Blockchain Federal Argentina.

Debe resaltarse que la innovación clave de este modelo radica en el denominado “anclaje” o consolidación periódica, mediante la cual tras un tiempo determinado (cada hora o al final del día), el *hash* de todas las transacciones de la *Layer 2* se agrupará en una única transacción, y se registraría en la *Layer 1* de Cardano. Las ventajas de este modelo radican en la velocidad de la operatoria diaria y en los costos operacionales drásticamente reducidos. Además, la integridad de todos los registros queda sellada de forma inmutable en la red pública de Cardano, auditable por cualquier ciudadano o parte del proceso.

En cuarto lugar, para mayor claridad debería establecerse un Protocolo Unificado de Incorporación de Evidencia. Esto implicaría que la ley debería establecer un protocolo técnico obligatorio para la incorporación de evidencia digital por parte de las fuerzas de seguridad y peritos oficiales. Dicho protocolo debe ordenar que, al momento de recolectar una prueba digital (por ejemplo, la pericia de un teléfono o el secuestro de correos electrónicos), el software oficial utilizado debería automáticamente: Calcular el valor *hash* de la evidencia, almacenar la evidencia original en un repositorio judicial seguro, y registrar en

la *blockchain* una transacción que contenga el valor *hash*, el ID de la causa, el ID del funcionario, el tipo de prueba y el sello de tiempo (timestamp).

Por último, debe establecerse el principio de Confidencialidad Off-Chain. La ley debe ser explícita en que la *blockchain* sólo almacenará metadatos y *hashes*. La evidencia en sí misma (el contenido) permanecerá fuera de la cadena (off-chain), en los repositorios seguros, y su acceso estará regido por las normas procesales vigentes sobre publicidad, secreto de sumario y protección de datos personales.

Una propuesta de esta índole resulta crucial, puesto que su implementación no sólo resolvería las vulnerabilidades del sistema actual de custodia, como las vistas en el caso "Vélez Cheratto", sino que otorgaría a la justicia argentina una herramienta técnica que garantiza la integridad probatoria, pilar fundamental del debido proceso.

**Conclusiones**

La presente investigación partió de una pregunta central: ¿Puede la tecnología *blockchain* mejorar el resguardo de las evidencias? La investigación permite afirmar una respuesta contundente: sí, y la necesidad de su implementación es urgente.

Se ha demostrado que las vulnerabilidades expuestas en casos como "Ricardo Jaime" o "Vélez Cheratto" no son anomalías, sino síntomas de un sistema de custodia diseñado para la evidencia física, que resulta insuficiente para la naturaleza volátil de la prueba digital.

La solución, sin embargo, no requiere de la invención de un nuevo medio de prueba, sino de aplicar una herramienta de conservación o resguardo superior. Esta distinción conceptual es la clave del análisis y ya ha sido validada por un caso de jurisprudencia nacional en el fallo "Ruiz Solís, Gabriel de Jesus C/ Berruete, Andrea Viviana", que reconoció la capacidad de la *blockchain* (en este caso, la BFA) para probar la integridad y fecha cierta de un documento, separándola de la valoración de su contenido.

El análisis del derecho comparado (China y EE.UU.) demuestra que la adopción de esta tecnología es una realidad jurídica global. A su vez, el hito del primer contrato ejecutable en Cardano en Argentina prueba que esta red, con su arquitectura enfocada en la seguridad, ya está produciendo efectos jurídicos en nuestro país.

Por todo lo expuesto, esta investigación concluye que el camino más seguro y eficiente no es una red permisionada y centralizada, sino el modelo híbrido propuesto: una sidechain o *Layer 2* de operatoria judicial (veloz y confidencial) "anclada" a la *Layer 1* pública de Cardano, que garantiza la máxima integridad y auditabilidad pública.

La respuesta a la hipótesis es, por tanto, afirmativa. Su implementación para fortalecer el debido proceso es viable. No obstante, tal como se sostuvo, exige un marco claro que se asiente sobre tres premisas transversales: la definición normativa de la tecnología, otorgando presunción *iuris tantum* al *hash* registrado; la garantía absoluta de confidencialidad mediante el modelo *off-chain* para resolver las tensiones con la Ley de Protección de Datos Personales; y el aseguramiento de una gobernanza descentralizada mediante la distribución de los nodos validadores entre los actores clave del sistema judicial.

En definitiva, la incorporación de la *blockchain* a la cadena de custodia constituye una necesidad jurídica imperativa para asegurar mayor integridad, transparencia y auditabilidad en los procesos judiciales. Si bien la comunidad internacional ya ha sentado las bases, el Estado Argentino cuenta con los cimientos conceptuales y tecnológicos idóneos para su ejecución. En este sentido, el modelo propuesto posee la capacidad de subsanar las vulnerabilidades estructurales del sistema actual.

En suma, se trata de una solución compatible con el marco normativo vigente, respetuosa de la confidencialidad y alineada con los estándares internacionales. De esta forma, la tecnología no viene a reemplazar al sistema jurídico, sino a fortalecerlo de manera simultánea. Su implementación, bajo los pilares enunciados, representa el camino más idóneo para consolidar un sistema probatorio a la altura de los desafíos del Siglo XXI.

**Bibliografía**

Agüero, A. y Piottante, R. (2023, 18 de diciembre). *Transformación digital. Cadena de custodia de evidencias digitales*. Secretariado Permanente de Tribunales de Cuentas, Órganos y Organismos Públicos de Control Externo de la República Argentina. Tribunal de Cuentas de la provincia de Mendoza. https://tribunalesdecuentas.org.ar/congreso-2022-san-luis-3/

Artica, D. (2024, 11 de diciembre). *Los retos que enfrenta la adopción de blockchain: ¿Qué es y cómo puede impactarnos?*. Moventi. https://www.linkedin.com/pulse/los-retos-que-enfrenta-la-adopci%C3%B3n-de-blockchain-qu%C3%A9-es-y-aw9xe/

Baidu (2019, 21 de febrero). *Baidu Announces Fourth Quarter and Fiscal Year 2018 Results*. https://ir.baidu.com/news-releases/news-release-details/baidu-announces-fourth-quarter-and-fiscal-year-2018-results/

Bartolomeo, A., Machin, G., Capello, B., Garay, M., Mamaní, D., Yacante, L. (2020). *Introducción a la tecnología blockchain: Su impacto en las ciencias económicas*. Universidad Nacional de Cuyo. https://bdigital.uncu.edu.ar/fichas.php?idobjeto=15304

Blanco, L. (2018, 1 de noviembre). *Escena del crimen y cadena de custodia: Análisis (comparativo) de parte de la normativa sudamericana y argentina*. Revista Pensamiento Penal. https://www.pensamientopenal.com.ar/system/files/2018/11/doctrina47102.pdf

Blockchain Federal Argentina. (s.f.). *Aplicaciones*. https://bfa.ar/bfa/aplicaciones

Blockchain Federal Argentina. (s.f.). *Cómo funciona*. https://bfa.ar/bfa/como-funciona

Blockchain Federal Argentina. (s.f.) *Infraestructura*. https://bfa.ar/bfa/infraestructura

Cámara de Apelación en lo Civil y Comercial de Morón (Argentina), Sala II. (2024). *Ruíz Solís, Gabriel de Jesús c/Berruete, Andrea Viviana, Herederos de Ventimiglia y Otros s/ Daños y Perj. Autom. c/ Les. o Muerte* (Exc. Estado). (Expte. N° MO-5892-2022). SAIJ. https://www.saij.gob.ar/camara-apelaciones-civil-comercial-local-buenos-aires--herederos-otro-danos-perj-autom-les-muerte-exc-estado-fa24010011-2024-02-22/123456789-110-0104-2ots-eupmocsollaf

Cámara Federal de Casación Penal (argentina), Sala I. (2018, 27 de junio). *Vélez Cheratto, Emanuel s/ recurso de casación*. SAIJ. https://www.saij.gob.ar/camara-federal-casacion-penal-federal-ciudad-autonoma-buen

os-aires-velez-cheratto-emanuel-recurso-casacion-fa18260276-2018-06-27/123456789-672-0628-1ots-eupmocsollaf

Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal (Argentina), Sala I. (2012, 24 de mayo). *Fiscal s/ apela declaración de nulidad de informe pericial - Ricardo Jaime* (Causa N° 46.744). https://www.csjn.gov.ar/archivo-cij/nota-9170-La-Camara-Federal-confirmo-la-anulacion-de-peritaje-sobre-mails-en-causa-contra-Ricardo-Jaime-.html

Comisión de Derecho Internacional (Organización de las Naciones Unidas). (1969, 23 de mayo). *Convención de Viena sobre el Derecho de los Tratados.* derechos.org. https://www.derechos.org/nizkor/ley/viena.html

Congreso de la Nación (Argentina). (2000, 4 de octubre). *Ley 25.326. Protección de Datos Personales.* INFOLEG. https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

Congreso de la Nación (Argentina). (2017, noviembre). *Ley 27.411. Aprobación del Convenio sobre Ciberdelito. (Convenio de Budapest)*. INFOLEG. https://servicios.infoleg.gob.ar/infolegInternet/anexos/300000-304999/304798/norma.htm

Consejo de Europa. (2001, 23 de noviembre). *Convenio sobre la Ciberdelincuencia (Convenio de Budapest, ETS n.º 185) y sus Protocolos*. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Corti, J. (2025, 23 de octubre). *La investigación penal en la era digital: desafíos en vías de una persecución eficiente de la criminalidad*. Zona Gris - Newsletter CIPCE #1 (Instituto de Estudios Comparados en Ciencias Penales y Sociales). https://inecip.org/noticias/la-investigacion-penal-en-la-era-digital-desafios-en-vias-de-una-persecucion-eficiente-de-la-criminalidad/

Gaiardo, D. (2018). *Uso de la tecnología para mejorar la cadena de custodia*. Premio REFLEJAR - Las nuevas tecnologías en el servicio de justicia. https://latam.ijeditores.com/pop.php?option=articulo&Hash=6d199542bd7a3f2a0397da70c3128767&from_section=relacionados

García Hernandez, J. (2018, junio). *Criptomonedas y Aplicación en la Economía*. Universidad Pontificia Comillas Madrid. https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/32886/TFM001066.pdf?sequence=1

Grosso Molina, G. (2023, 13 de junio). *Nuevas tecnologías: blockchain, criptoactivos y smart contracts (II[a] parte). Efectos de su uso en las relaciones privadas y encuadre jurídico.* Editores Fondo Editorial. https://ar.ijeditores.com/pop.php?option=articulo&Hash=2f530d4eccc860c1f098cc1b5c32f380

Harkavy, R. (2024, 11 de octubre). *Smart contracts come to Argentina.* Global Legal Insights. https://www.globallegalinsights.com/news/smart-contracts-come-to-argentina/

Hoskinson, C. (2017). *Why Cardano: Designing in Layers.* IOHK. https://why.cardano.org/en/introduction/designing-in-layers/

Jara, M. (2022, 1 de septiembre). *Blockchain y derecho. Un abordaje preliminar.* Colegio de Abogados de Morón (CAM). https://ijeditores.com/pop.php?option=articulo&Hash=64ad6f35f7ea3bb6d50c7b51fbf9da76

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2019). *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol*. Springer International Publishing. https://eprint.iacr.org/2016/889.pdf

Lavin Perrino, I. & Llanos Ferraris, D. (2025). *An Analysis of Blockchain Solutions for Digital Evidence Chain of Custody.* Universidad de Valladolid. Repositorio documental. https://uvadoc.uva.es/bitstream/handle/10324/75760/_blockchain_2025_Chain_of_custody_under_iso.pdf?sequence=1&isAllowed=y

Massina, L. (2024, 10 de octubre). *Hito Histórico: Primer Contrato Legalmente Exigible en la Red de Cardano Firmado en Argentina*. criptotendencias.com. https://www.criptotendencias.com/actualidad/hito-historico-primer-contrato-legalmente-exigible-en-la-red-de-cardano-firmado-en-argentina/#google_vignette

Melo, L. (2019). *Régimen jurídico de blockchain: una prueba atípica*. Revista de Bioética y Derecho, (46), 101-116. http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872019000200007&lng=es&tlng=es.

Ministerio Público Fiscal (Argentina). (2015, julio). *Manual de procedimientos del sistema de cadena de custodia*. mpf.gob.ar. https://www.mpf.gob.ar/capacitacion/files/2015/07/Cadena-de-Custodia.pdf

Ministerio Público Fiscal & Ministerio Público de la Defensa (Argentina). (2023). *Protocolo para la identificación, recolección, preservación, procesamiento y presentación de*

*evidencia digital*. fiscales.gob.ar. https://www.fiscales.gob.ar/wp-content/uploads/2023/04/MINSEG-MPFN-Protocolo-evidencia-digital-2.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press. https://books.google.com.ar/books/about/Bitcoin_and_Cryptocurrency_Technologies.html?id=LchFDAAAQBAJ&redir_esc=y#:~:text=It%20begins%20by%20tracing%20the%20history%20and%20development,integrate%20ideas%20from%20Bitcoin%20into%20your%20own%20projects.

Pérez Campillo, L. (2025, marzo). *Implementación de blockchain en el sistema judicial público y en los ADR.* Universidad Europea de Madrid. https://raco.cat/index.php/IDP/article/view/429135/526615

Presidencia de la Nación (Argentina). (1972, 10 de octubre). *Ley 19.836 de Aprobación de la Convención de Viena sobre el Derecho de los Tratados.* INFOLEG. https://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/217116/norma.htm

Presidencia de la Nación (Argentina). (2017, 15 de julio). *Certificación con Blockchain.* boletinoficial.gob.ar. https://www.boletinoficial.gob.ar/estatica/certificacion-blockchain

Presidencia de la Nación (Argentina). (2023, 20 de diciembre). Decreto 70/2023. *Bases para la reconstrucción de la economía argentina.* https://www.boletinoficial.gov.ar/detalleAviso/primera/301122/20231221

Renzullo, J., Pineda, A., Oliveros, J., & Díaz, A. (2023). *Manual de Blockchain. Cadena de bloques y tecnología. Herramienta para la transparencia y el fortalecimiento institucional para sector público, privado y sociedad civil.*. Cedice Futuro. https://libreriacedice.org.ve/wp-content/uploads/2023/11/manualblockchain23.pdf

Sosa, M. (2023, 11 de mayo). *Evidencia digital: Su importancia en la investigación . Revista Pensamiento Penal*. https://www.pensamientopenal.com.ar/system/files/Documento_Editado1140.pdf

State of Illinois (101st General Assembly). (2020). *Blockchain Technology Act. Public Act 101-0513.* https://www.ilga.gov/documents/legislation/101/HB/10100HB3575.htm

The Supreme People's Court of The People's Republic of China. (2019, 4 de diciembre). *Hangzhou Huatai Media Culture Media Co., Ltd. v. Shenzhen Daotong Technology*

*Development Co., Ltd.* (Case of Dispute over Right of Dissemination over Internet). Rule Of Law in Internet: Cases. https://english.court.gov.cn/2019-12/04/c_766707.htm

Tribunal Supremo (España), Sala Segunda. (2019, 20 de junio). *STS 326/2019*. vLEX. https://vlex.es/vid/797938401

Voshmgir, S. (2020). *Token Economy: How the Web3 reinvents the Internet.* Token Kitchen. https://token.kitchen/token-economy/third-edition

Wang, Z. (2021). *China's E-Justice Revolution. Judicature* (Bolch Judicial Institute at Duke Law). https://judicature.duke.edu/wp-content/uploads/sites/3/2021/04/EJustice_Spring2021-1.pdf

Zou, L. & Chen, D. (2024, 9 de septiembre). *Using Blockchain Evidence in China's Digital Copyright Legislation to Enhance the Sustainability of Legal Systems*. MPDI Open Access Journal Systems. https://doi.org/10.3390/systems12090356