REGULACIÓN DE LA CADENA DE BLOQUES (*BLOCKCHAIN*) EN EL CÓDIGO NACIONAL DE PROCEDIMIENTOS CIVILES Y FAMILIARES

REGULATION OF BLOCKCHAIN IN THE NATIONAL CODE OF CIVIL AND FAMILY PROCEDURES

Julia RUIZ BUZO*
https://orcid.org/0009-0007-0418-6585
https://doi.org/10.5281/zenodo.18623117

Resumen: La cadena de bloques puede ser comprendida como una tecnología basada en una arquitectura de red abierta, descentralizada y distribuida, que posibilita el registro inalterable de transacciones mediante el empleo de mecanismos criptográficos avanzados, funciones *hash,* sellos de tiempo (*timestamp*), y algoritmos de consenso. Esta configuración técnica garantiza, la autenticidad, integridad y no repudio de los datos registrados. Por sus elevados estándares de seguridad para el registro, conservación y trazabilidad de mensajes de datos, esta tecnología ha sido reconocida por el Código Nacional de Procedimientos Civiles y Familiares (CNPCF) como un medio tecnológico apto para su utilización en el contexto de la justicia digital, tanto como medio de prueba, como para el resguardo de expedientes electrónicos.

No obstante, para que los mensajes de datos almacenados en una cadena de bloques gocen de pleno valor probatorio ante las autoridades jurisdiccionales,

* Profesora de cátedra de la Facultad de Derecho y RRII de la Universidad Anáhuac Mayab. Contacto: juliarbuzo@buzoasociados.com

deben observarse los requisitos establecidos por dicho ordenamiento, los cuales son compatibles con lo dispuesto por la Norma Oficial Mexicana NOM-151-SCFI-2016.

A fin de lograr la adecuada admisión, desahogo y valoración de las pruebas digitales sustentadas en tecnología *blockchain*, es imprescindible acreditar, el proceso de generación, conservación, autenticación y acceso del mensaje de datos correspondiente. Además de que proveer los medios técnicos idóneos para su consulta, análisis y valoración, en virtud de que la mayoría de los órganos jurisdiccionales aún no cuenta con las herramientas informáticas necesarias para verificar este tipo de evidencia digital.

Palabras clave: Cadena de bloques, sello de tiempo, tecnologías de la información, nodos, mensajes de datos, justicia digital.

Abstract: Blockchain technology may be understood as a technological infrastructure based on an open, decentralized, and distributed network architecture, which enables the immutable recording of transactions through the use of advanced cryptographic mechanisms, hash functions, timestamps, and consensus algorithms. This technical configuration ensures the authenticity, integrity, and non-repudiation of the recorded data.Due to its high standards of security for the recording, preservation, and traceability of data messages, this technology has been expressly recognized by the National Code of Civil and Family Procedure (CNPCF) as a suitable technological means for its use within the framework of digital justice, both as a means of evidence and for the safekeeping of electronic case files. However, in order for data messages stored on a blockchain to be granted full evidentiary value before judicial authorities, they must comply with the procedural and technical requirements established by said Code, which are consistent with the provisions set forth in the Mexican Official Standard NOM-151-SCFI-2016. To ensure the proper admission, presentation, and assessment of digital evidence based on blockchain technology, it is essential to demonstrate, in a clear and technically verifiable manner, the process of

generation, preservation, authentication, and access of the corresponding data message. In addition, the technical means necessary for the consultation, analysis, and evaluation of such evidence must be duly provided, considering that the vast majority of judicial bodies do not yet possess the technological tools required to verify this type of digital evidence.

Keywords: Blochchain, time of stamp, information technologies, nodes, data messages, digital justice o e-justice.

I. Introducción

El siglo XXI se ha caracterizado por un desarrollo exponencial de las tecnologías emergentes. Klaus Schwab[1], en su libro "La cuarta revolución industrial", destaca innovaciones como la inteligencia artificial (IA), la robótica, el internet de las cosas (IoT), los vehículos autónomos, la impresión 3D, la nanotecnología, la biotecnología, la ciencia de materiales, el almacenamiento de energía y la computación cuántica.

Resulta evidente que estos avances han permeado todos los ámbitos de la vida humana, y en particular, han transformado profundamente las formas de comunicación. El derecho de libertad de expresión y el derecho a la información se han visto impactados significativamente por el uso de las tecnologías de la información y la comunicación (TIC).

La Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, en su artículo 29 Quárter define a las TIC como: "Aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos". [2]

Dentro del espectro de las tecnologías de la información, se encuentran dispositivos y herramientas como computadoras, softwares, redes, servidores y más recientemente, la tecnología *blockchain* (cadena de bloques). Por su parte,

[1] Schwab, Klaus, "La cuarta revolución industrial", México, *Penguin Random House*, 2017, p, 13.
[2] La Ley General de Acceso de las Mujeres a una Vida Libre de Violencia Artículo 29 Quáter, disponible en *https://www.diputados.gob.mx/LeyesBiblio/pdf/LGAMVLV.pdf* (04 de agosto de 2025).

las tecnologías de la comunicación comprenden herramientas como el correo electrónico, videoconferencias, redes sociales, telefonía móvil, internet y televisión digital.

En el ámbito del derecho privado, los profesionales del derecho han incorporado herramientas tecnológicas (*legal tech*) para optimizar la prestación de servicios legales. En el ámbito del derecho público, dichas tecnologías se han implementado progresivamente en la administración de justicia, con la finalidad de modernizar y optimizar los procesos jurisdiccionales, fenómeno al que se conoce como *e-justice*, o justicia digital.

En este contexto y conforme a la definición de justicia digital propuesta por Medina, esta puede entenderse como "la aplicación interna y externa de cualquier tipo de tecnología digital en la preparación, sustanciación, resolución y ejecución de los procedimientos seguidos en forma de juicio, con la finalidad de eficientizar la administración de justicia".[3]

La exposición de motivos del Código Nacional de Procedimientos Civiles y Familiares (CNPCF) evidencia la voluntad del legislador de "aprovecha las herramientas de la tecnología de la información [y la comunicación,] para garantizar mayor acceso a la justicia en la solución de conflictos".[4]

Antes de la pandemia de COVID-19, el uso de las TIC en los procesos judiciales mexicanos era incipiente. A partir del 2000, órganos como el Consejo de la Judicatura Federal y diversos tribunales estatales, desarrollaron plataformas digitales para audiencias virtuales, presentación de demandas y notificaciones electrónicas, como el Sistema Integral de Seguimiento de Expedientes (SISE) y el Sistema Electrónico de Gestión Judicial (SEGEJ).

[3] Medina, Zepeda, Emmanuel, "Hacia una teoría de la *e justice* o justicia digital: instrucciones para armar", Revista Mexicana de Derecho Constitucional, México, núm 46, enero-junio 2022, p,178, disponible en *https://revistas.juridicas.unam.mx/index.php/cuestiones-constitucionales/article/view/17052/17596,* (04 de agosto de 2024)

[4] Cámara de Diputados, Iniciativa con proyecto de decreto por el que se expide el Código Nacional de Procedimientos Civiles y Familiares, 8 de febrero de 2022, p, 6, *disponible en https://infosen.senado.gob.mx/sgsp/gaceta/65/1/2021-12-02-1/assets/documentos/Inic_Morena_Sen_Moreal_Menchaca_Expide_Codigo_Nacional_Procedimiento_Civiles_Familiares.pdf* (04 de agosto de 2025).

La crisis sanitaria evidenció que el uso de las TIC no era solo conveniente sino indispensable. El colapso temporal del sistema judicial reveló la urgente necesidad de una transformación digital profunda. El Índice de Estado de Derecho del *World Justice Project*[5], posicionó a México en el lugar 116 de 128 países evaluados en 2020, señalando la ausencia de justicia digital como uno de los principales obstáculos al acceso efectivo de la justicia.

Uno de los factores que contribuyó a esta deficiencia fue la falta de una regulación uniforme tanto a nivel federal como local que permitiera la incorporación sistemática y segura de herramientas digitales en todo el país.

El 7 de junio de 2023, se publicó en el Diario Oficial de la Federación el nuevo Código Nacional de Procedimientos Civiles y Familiares[6] (CNPCF), cuya entrada en vigor será en el ámbito federal, a más tardar el 1 de abril de 2027; y en los estados, en la fecha que cada Congreso local determine, sin rebasar dicho límite.[7]

Este ensayo tiene como objetivo analizar el tratamiento jurídico que el CNPCF otorga a la tecnología *blockchain* como mecanismo de registro, conservación y validación de mensajes de datos en el ámbito procesal civil y familiar, con énfasis en su eficacia probatoria y su compatibilidad con la NOM-151-SCFI-2016[8].

El trabajo se estructura en tres capítulos: el primero desarrolla una conceptualización técnica y jurídica de la tecnología *blockchain* y sus aplicaciones potenciales en los sistemas judiciales contemporáneos; el segundo examina detalladamente el marco normativo del CNPCF, enfocándose en la admisión de esta tecnología como medio de prueba, sus requisitos de validez y sus implicaciones dentro del nuevo paradigma del juicio en línea. El capítulo, aborda

[5] WORLD JUSTICE PROJECT, Hallazgos principales del Índice de Estado de Derecho en México 2020-2021: Resultados destacados y tendencias, 2021, p. 26, *https://worldjusticeproject.mx/wp-content/uploads/2021/04/3_mx-insights-ESP.pdf,* (04 de agosto de 2024).

[6] Código Nacional de Procedimientos Civiles y Familiares, disponible en https*://www.diputados.gob.mx/LeyesBiblio/pdf/CNPCF.pdf,* (10 de julio de 2024).

[7] Art. 3º., Código Nacional de Procedimientos Civiles y Familiares, *op, cit.*

[8] Norma Oficial Mexicana NOM-151-SCFI-2016, disponible en https://www.dof.gob.mx/normasOficiales/6499/seeco11_C/seeco11_C.html (5 de agosto de 2025)

de manera tangencial, otros usos de la cadena de bloques en el ámbito de la administración de justicia, como su empleo para resguardar información dentro de un juicio en línea, y su implementación dentro del arbitraje como medio alternativo de solución de controversias.

II. La cadena de bloques (*blockchain*).

2.1De la justicia tradicional a la justicia digital.

El artículo 17[9] de la Constitución Política de los Estados Unidos Mexicanos, contempla el derecho fundamental de acceso a la justicia, entendido como un derecho instrumental que permite garantizar y a hacer efectivo otros

[9] Artículo 17: "Ninguna persona podrá hacerse justicia por sí misma, ni ejercer violencia para reclamar su derecho.
Toda persona tiene derecho a que se le administre justicia por tribunales que estarán expeditos para impartirla en los plazos y términos que fijen las leyes, emitiendo sus resoluciones de manera pronta, completa e imparcial. Su servicio será gratuito, quedando, en consecuencia, prohibidas las costas judiciales. Las leyes preverán las cuantías y supuestos en materia tributaria en las cuales tanto los Tribunales Administrativos como las Juezas y Jueces de Distrito y Tribunales de Circuito del Poder Judicial de la Federación o, en su caso, la Suprema Corte de Justicia de la Nación, deberán resolver en un máximo de seis meses, contados a partir del conocimiento del asunto por parte de la autoridad competente. En caso de cumplirse con el plazo señalado y que no se haya dictado sentencia, el órgano jurisdiccional que conozca del asunto deberá dar aviso inmediato al Tribunal de Disciplina Judicial y justificar las razones de dicha demora o, en su caso, dar vista al órgano interno de control tratándose de Tribunales Administrativos.
Siempre que no se afecte la igualdad entre las partes, el debido proceso u otros derechos en los juicios o procedimientos seguidos en forma de juicio, las autoridades deberán privilegiar la solución del conflicto sobre los formalismos procedimentales.
El Congreso de la Unión expedirá las leyes que regulen las acciones colectivas. Tales leyes determinarán las materias de aplicación, los procedimientos judiciales y los mecanismos de reparación del daño. Los jueces federales conocerán de forma exclusiva sobre estos procedimientos y mecanismos.
Las leyes preverán mecanismos alternativos de solución de controversias. En la materia penal regularán su aplicación, asegurarán la reparación del daño y establecerán los casos en los que se requerirá supervisión judicial.
Las sentencias que pongan fin a los procedimientos orales deberán ser explicadas en audiencia pública previa citación de las partes.
Las leyes federales y locales establecerán los medios necesarios para que se garantice la independencia de los tribunales y la plena ejecución de sus resoluciones.
La Federación y las entidades federativas garantizarán la existencia de un servicio de defensoría pública de calidad para la población y asegurarán las condiciones para un servicio profesional de carrera para los defensores. Las percepciones de los defensores no podrán ser inferiores a las que correspondan a los agentes del Ministerio Público.
Nadie puede ser aprisionado por deudas de carácter puramente civil", disponible en *https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf,* (28 de julio del 2025).

derechos humanos.

La Corte Interamericana de Derechos Humanos (CIDH)[10], ha interpretado que este derecho implica la obligación estatal de prever recursos efectivos que permitan la protección de los derechos establecidos en la ley, y de instaurar tribunales que, conforme al principio de legalidad, impartan justicia de manera pronta, expedita, imparcial, gratuita y con la capacidad de ejecutar sus resoluciones.

El auge de las tecnologías de la información y comunicación (TIC) han transformado la interacción social, lo que ha impactado directamente en la manera de impartir justicia. Los actos jurídicos que se generan y conservan a través de medios digitales requieren, por tanto, de una regulación que garantice su admisibilidad, autenticidad y eficacia probatoria ante los tribunales.

En este contexto, la Ley Modelo de la CNUDMI sobre Comercio Electrónico (MLEC, 1996), adoptada por México, fue pionera en reconocer la equivalencia funcional entre documentos en papel y mensajes de datos. En su artículo 8º[11] establece los requisitos que debe cumplir un mensaje de datos para ser considerado como documento original; el artículo 9º[12] regula su admisibilidad y fuerza probatoria;

[10] CIDH, Cuadernillo de Jurisprudencia de la Corte Interamericana de Derechos Humanos, núm 13, Derecho a la Justicia, San José de Costa Rica, 2021, disponible en *https://www.corteidh.or.cr/sitios/libros/todos/docs/cuadernillo13_2021.pdf* (04 de agosto de 2024).

[11] Artículo 8. — Original

"1) Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos:

a) Si existe alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma;

b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar.

2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no sea presentada o conservada en su forma original.

3) Para los fines del inciso a) del párrafo 1):

a) La integridad de la información será evaluada conforme al criterio de que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de su comunicación, archivo o presentación; y

b) El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso. 4) Lo dispuesto en el presente artículo no será aplicable a: [...]"

[12] Artículo 9. — "Admisibilidad y fuerza probatoria de los mensajes de datos.

1) En todo trámite legal, no se dará aplicación a regla alguna de la prueba que sea óbice para la

y el artículo 10º[13] determina las condiciones para su conservación. Tales exigencias se alcanzan mediante tecnologías que aseguren la integridad, inalterabilidad y recuperabilidad de la información, como lo es la cadena de bloques.

La tecnología *blockchain,* al ser un sistema descentralizado, criptográficamente seguro e inmutable, ha sido reconocida en el nuevo Código Nacional de Procedimientos Civiles y Familiares (CNPCF) como medio idóneo para la generación y conservación de mensajes de datos con valor probatorio pleno, conforme a lo dispuesto en los artículos 348, 349 y 350 del propio ordenamiento. Asimismo, su uso debe observar los requisitos técnicos establecidos por la Norma Oficial Mexicana NOM-151-SCFI-2016[14] y, en su caso, por la Ley de Firma Electrónica Avanzada[15].

El CNPCF marca un hito al establecer los parámetros normativos y técnicos que permiten considerar como originales los documentos generados y conservados

admisión como prueba de un mensaje de datos:
2)
a) Por la sola razón de que se trate de un mensaje de datos; o
b) Por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.
3) Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente."

[13] Artículo 10. — "Conservación de los mensajes de datos
1) Cuando la ley requiera que ciertos documentos, registros o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las condiciones siguientes:
a) Que la información que contengan sea accesible para su ulterior consulta; y
b) Que el mensaje de datos sea conservado con el formato en que se haya generado, enviado o recibido o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida; y
c) Que se conserve, de haber alguno, todo dato que permita determinar el origen y el destino del mensaje, y la fecha y la hora en que fue enviado o recibido.
2) La obligación de conservar ciertos documentos, registros o informaciones conforme a lo dispuesto en el párrafo 1) no será aplicable a aquellos datos que tengan por única finalidad facilitar el envío o recepción del mensaje.
3) Toda persona podrá recurrir a los servicios de un tercero para observar el requisito mencionado en el párrafo 1), siempre que se cumplan las condiciones enunciadas en los incisos a), b) y c) del párrafo 1)"

[14] NOM-151-SCFI-2016, *op. Cit.*

[15] Ley de Firma Electrónica Avanzada, disponible en https://www.diputados.gob.mx/LeyesBiblio/pdf/LFEA_200521.pdf (5 de agosto de 2025)

en *blockchain,* siempre que se cumplan condiciones como el uso de firmas electrónicas avanzadas, *hash* criptográfico, sello de tiempo (*timestamp*), metadatos verificables, y plataformas compatibles con redes públicas y descentralizadas. Con ello, México fortalece su modelo de justicia digital, avanzando hacia la consolidación de un sistema jurisdiccional moderno, accesible y tecnológicamente robusto, que garantiza tanto la autenticidad como la integridad de los documentos electrónicos.

La incorporación de estas herramientas tecnológicas responde al mandato constitucional de garantizar un acceso efectivo a la justicia, eliminando barreras físicas, geográficas o tecnológicas, y cumpliendo con los principios de legalidad, seguridad jurídica y debido proceso.

En lo sucesivo, este capítulo desarrollará las definiciones, características y clasificaciones de la cadena de bloques, así como su impacto y aplicación concreta en los procesos judiciales contemplados por el CNPCF.

2.2 Definición de la cadena de bloques

En el año 2008 se publicó en internet el documento técnico (*white paper*) de Bitcoin, firmado por Satoshi Nakamoto (seudónimo), quien, mediante una red distribuida y pública denominada *"blockchain",* hizo posible la compraventa digital de la criptomoneda "Bitcoin". En palabras de expertos, "el hito más relevante en el mundo de los sistemas distribuidos es la publicación del *white paper* de Bitcoin*"*[16].

Posteriormente, en 2014, se desarrolló Ethereum[17], una *blockchain* que, además de permitir la compraventa de la criptomoneda Ether, posibilitó el registro de transacciones complejas. "Ethereum añade una capa de procedimientos almacenados *(smart contracts)* que permiten insertar lógica de negocio en la red, la cual, una vez desplegada, no puede modificarse"[18].

[16] Martínez, José y Coloma, Juan Carlos. *How blockchain and smart contracts have change how we do business: legal perspective,* en Gurrea, A., (eds), *Blockchain, fintech and law*, Valencia, *Tirant lo blanch*, 2022, p 23.

[17] Para abundar en la información de *Ethereum* acceder a *https://ethereum.github.io/yellowpaper/pap*, (24 junio de 2024).

[18] González, A. *Blochchain, Curso superior en derecho: aspectos jurídicos de los smart contracts y blockchain*, Plataforma Universidad de Salamanca/Doinglobal, (en línea), 2023.

Ambas redes comparten como base la tecnología blockchain. Al respecto, Martínez y Coloma la definen como "una estructura de datos gobernada por un sistema distribuido con un número indeterminado de participantes, que opera mediante un proceso específico de consenso y utiliza identificación criptográfica"[19].

Por su parte, el jurista mexicano David Merino la conceptualiza como "una estructura de datos en la que la información contenida se agrupa en bloques, a los cuales se añade metainformación relativa al bloque anterior dentro de una línea temporal; y que, mediante técnicas criptográficas, impide la edición o repudio de la información salvo que se modifiquen todos los bloques posteriores"[20].

La magistrada Yolanda Ríos se refiere a ella como "una base de datos descentralizada, basada en la tecnología de registro distribuido (DLT), en la que múltiples nodos o usuarios, mediante el sistema *peer-to-peer*, validan la información registrada en cada bloque conforme a una fórmula de consenso, bastando que el acuerdo se adopte por mayoría para que la información se considere fiable y auténtica"[21].

Asimismo, Alfonso Delgado aclara que el término *blockchain* se utiliza en ocasiones como sinónimo de "tecnología de registros distribuidos"[22], (DLT, por sus siglas en inglés).

En consecuencia, la cadena de bloques puede entenderse como una tecnología sustentada en una red abierta, descentralizada y distribuida, que permite el registro inalterable de transacciones mediante el uso de mecanismos criptográficos, funciones de *hash*, sellos de tiempo *(timestamp),* metadatos verificables, y métodos de consenso, garantizando así la autenticidad e integridad de los datos registrados.

---

[19] Martínez, José y Coloma Juan, *op. cit,.* p.23.
[20] Merino, David, *Blockchain, Introducción al derecho tecnológico*, México, Juristech, 2019, p,139.
[21] Ríos, Yolanda. "Blockchain, smart contracts y administración de justicia", *Blochchain inteligence,* España, enero de 2021, disponible en *https://blockchainintelligence.es/wp-content/uploads/2021/02/BLOCKCHAIN-SMART-CONTRACTS-Y-ADMINISTRACION-DE-JUSTICIA_YOLANDA-RIOS.pdf* (28 de julio de 2025).
[22] Delgado, Alfonso. *Blockchain:concepto, funcionamiento y aplicaciones*. Valencia, *Tirant lo blanch*, 2020, p.32.

2.3 Características de la tecnología *blockchain*.

La mejor manera de entender un concepto tan complejo e innovador como la tecnología *blockchain*, es describiendo sus características principales.

Por otra parte, es necesario conocer las características de esta tecnología para comprender su funcionamiento y eficacia en el registro seguro de mensajes de datos, que pueden ser utilizados como pruebas en un juicio y que, si cumplen con los requisitos que marca el CNPCF serán considerados como pruebas plenas.

Existe consenso en la doctrina respecto de las características distintivas de la tecnología *blockchain,* las cuales se describen a continuación:

a) Abierta: cualquier persona puede acceder al sistema y al software, participando activamente en la creación y validación de la cadena de bloques.[23].

Esto implica una barrera significativa frente a posibles intentos de manipulación de la información registrada en *blockchain,* ya que cientos de usuarios, distribuidos globalmente y sin vínculos previos entre sí, participan en la validación de operaciones a través de nodos independientes. Tal dispersión impide alterar unilateralmente la información, asegurando que un mensaje de datos registrado en la *blockchain* sea archivado de manera segura para su ulterior consulta y verificación probatoria.

b) Pública: la red puede ser consultada por cualquier usuario, permitiendo la visualización de la trazabilidad completa de las operaciones registradas. No obstante, ello no implica el acceso al contenido sustantivo de la información, ya que ésta se encuentra cifrada mediante técnicas criptográficas avanzadas. En la red

[23] Por ejemplo, en México cualquier persona puede minar bitcoins, basta con adquirir un equipo computacional de gran potencia, bajar el software correspondiente a la criptomoneda que elijas y el hardware que uses y sumarte a un pool de minería ya que esta alternativa que puede ayudar a obtener mejores resultados, al combinan su potencia de procesamiento. "¿Cómo minar criptomonedas en México?: Guía simple de 6 pasos" (sitio web), Bitsoblog, México, 2023, disponible en *https://blog.bitso.com/es-mx/criptomonedas-mx/como-minar-criptomonedas-en-México,* (29 de julio de 2025).

solo se almacena el *hash*[24] de la operación, y no los datos sensibles. La identidad de las partes involucradas tampoco es visible, pues estas interactúan mediante mecanismos de firma electrónica asimétrica. Las partes, al ingresar al sistema, reciben en su "monedero" una firma electrónica que actúa como pseudónimo, con la cual operan. Los bloques que documentan las transacciones contienen dicha firma, pero no revelan la identidad del firmante[25].

Por esta razón, toda modificación a un documento electrónico registrado en *blockchain* resulta detectable, ya que la trazabilidad de las operaciones es pública. Cada registro validado y publicado contiene un *hash* vinculado al del bloque anterior, generando una secuencia verificable que permite confirmar la integridad del documento desde su creación, lo cual robustece su valor probatorio.

c) Descentralizada: la validación de las transacciones registradas no es realizada por una autoridad central, sino por una red interconectada de ordenadores, denominados "nodos", que conservan una copia completa de la cadena de bloques. Esta arquitectura descentralizada impide la pérdida de información como consecuencia de ciberataques o fallos en servidores centrales, otorgando así resiliencia a la red.

El mecanismo de validación más común es el denominado *proof of work* (PoW), basado en la teoría de juegos. Bajo este esquema, la computadora o nodo que primero resuelve un complejo algoritmo matemático propone la información a la red para su validación. Una vez que la mayoría de los nodos aprueba la operación, esta se registra y se publica en la cadena de bloques. El nodo que resuelve el

[24] Entendiéndose por *hash* "aquél que permite obtener un resultado de tamaño fijo a partir de una cantidad variable de información, generando un efecto que puede ser verificado posteriormente para garantizar que no se han producido cambios sobre los datos de entrada (cualquier mínimo cambio en la información sobre la que se aplica la función de *hash* obtiene un resultado completamente diferente). Además, es imposible inferir los datos de entrada conociendo el valor de *hash* generado a partir de ellos, ni siquiera generar un conjunto diferente de datos que permitan obtener el mismo valor de hash". González, A, Curso superior en derecho: aspectos jurídicos de los *smart contracts* y *blockchain,* Universidad de Salamanca/Doinglobal (en línea), 2023.

[25] Gorris, C, *Tecnología blockchain y contratos inteligentes. Inteligencia artificial*, Valencia, Tirant *lo blanch,* 2017, p. 152-195.

problema, denominado "minero", recibe una retribución en forma de criptomoneda (por ejemplo, bitcoin o ether).

Alfonso Delgado[26]. explica que este mecanismo de validación, mediante el cual un minero confirma un conjunto de transacciones pendientes, se conoce como *proof-of-work* (PoW). Los nodos participantes compiten periódicamente en una "carrera de minería" (*mining race*) para resolver un rompecabezas criptográfico. El nodo que encuentre un *input* que genere un *hash* válido obtiene el derecho de minar un nuevo bloque y recibir la recompensa correspondiente.

Cada transacción aprobada se registra mediante una huella digital (*hash),* la cual le confiere unicidad e inmutabilidad. Cada bloque contiene múltiples transacciones identificadas con sus respectivos *hashes*, y cada nuevo bloque se vincula al anterior mediante la inclusión del *hash* correspondiente. Esta estructura encadenada impide cualquier modificación, ya que alterar un bloque implicaría cambiar también los *hashes* subsiguientes, lo que sería detectado inmediatamente por los demás nodos.

En este sentido, los registros en *blockchain* son seguros, trazables e inalterables, atributos esenciales para su utilización como medio probatorio en juicio. Se debe verificar que cada operación derive de la anterior, creando una cadena ininterrumpida de transacciones validadas. La fortaleza del sistema reside en el sello cronológico (*hash*) y en el algoritmo matemático (*proof of work*).[27]"

Por lo tanto, modificar un registro requeriría un poder computacional extraordinario capaz de alterar simultáneamente la mayoría de los nodos de la red, lo que resulta prácticamente inviable. Solo un ataque que controlara más del 50% de los nodos podría comprometer el sistema, posibilidad que la comunidad técnica considera altamente improbable. Por ello, los mensajes de datos generados y conservados en *blockchain* aseguran su integridad desde el momento de su creación, lo que les otorga un elevado valor probatorio en sede judicial.

[26] Delgado, A, *op.cit*., p 32.
[27] Gorris, *op,cit*., p. 152-195.

d) Inmutable: la información registrada en la red no puede modificarse sin el consenso de la mayoría de los nodos, lo cual es sumamente improbable. Además, cualquier cambio alteraría el *hash,* permitiendo la detección inmediata de la modificación.

En este contexto, un mensaje de datos registrado en *blockchain* hace prueba de la fecha cierta en que fue creado, así como de su inalterabilidad, lo que aporta certeza jurídica en juicio.

e) Confidencial: aunque los registros pueden ser visualizados en la red, su contenido está encriptado y solo puede ser desencriptado mediante las claves públicas y privadas que poseen los usuarios autorizados, lo que garantiza la privacidad de la información.

f) Transparente: toda transacción queda grabada de manera permanente en la red, lo que permite acreditar con precisión la fecha y hora de su creación. *El hash* asociado a cada transacción incorpora estos datos, permitiendo a la autoridad jurisdiccional verificar con exactitud el momento en que fue generada la prueba digital.

g) Eficiente: la tecnología *blockchain* prescinde de intermediarios, lo que reduce costos y tiempos operativos, optimizando así los procedimientos judiciales y administrativos.

h) Segura: la información registrada no puede ser alterada ni eliminada, únicamente se puede adicionar nueva información. Asimismo, la red permite a los usuarios recuperar la información mediante sus claves de acceso, lo que garantiza su disponibilidad continua.

Todas estas características convierten a la tecnología *blockchain* en una infraestructura altamente confiable para la generación, conservación y resguardo de información electrónica, la cual puede ser utilizada en juicio con valor probatorio pleno, conforme a los artículos 348, 349 y 350 del Código Nacional de Procedimientos Civiles y Familiares, así como a lo dispuesto por la NOM-151-SCFI-2016 y la Ley de Firma Electrónica Avanzada.

2.4 Tipos de *blockchain*.

Es importante conocer los tipos de *blochchain* existentes, ya que no todas ellas proporcionan el mismo grado de seguridad en la generación y conservación de los mensajes de datos en ellas registradas.

Derivado del distinto grado de seguridad que ellas aportan, es que el CNPCF incluyó a la *blockchain* descentralizada, pública y no permisionada como la adecuada para el registro de los mensajes de datos que pueden llegar a tener un valor probatorio pleno en juicio.

a) Redes centralizadas y descentralizadas

Redes centralizadas: En este tipo de redes, como su nombre lo indica, existe una autoridad y un servidor central que controlan y regulan todas y cada una de las operaciones realizadas en dicha base de datos.

Una base de datos puede definirse como un conjunto de datos estructurados que se almacenan en un servidor. Las bases de datos centralizadas son gestionadas por un administrador central y se encuentran alojadas en un único servidor[28]. Por ejemplo, cuando realizamos una transferencia electrónica desde nuestra cuenta de cheques a otra cuenta, el banco —como autoridad central— controla la operación y determina si esta procede o no.

En la práctica, se ha evidenciado que las bases de datos centralizadas son vulnerables y proclives a fallas, resulta común experimentar caídas del sistema o sufrir ataques cibernéticos que comprometen cuentas e información personal. En este modelo de red, el usuario depende absolutamente de quien la controla. Existen múltiples intermediarios y se generan costos adicionales por comisiones. Además, las partes que interactúan en este sistema no se encuentran en condiciones de igualdad jurídica, lo cual puede derivar en abusos por parte de la autoridad central que rige la red.

[28] Delgado, A. *op, cit,* p. 33.

Redes descentralizadas: Este tipo de bases de datos surgieron precisamente como una reacción ante los excesos y limitaciones de las redes centralizadas, particularmente en el ámbito financiero. Tras la crisis del sistema bancario internacional en 2008, se propuso la creación de redes descentralizadas que no estuvieran sujetas a una autoridad central (como gobiernos o corporaciones), y en las que los usuarios participaran en condiciones de igualdad, bajo un esquema *"peer to peer",* tanto en la toma de decisiones como en la realización de operaciones[29].

El maestro Alfonso Delgado define a la base de datos distribuida como "un conjunto de múltiples bases de datos interrelacionadas y distribuidas a lo largo de una red de ordenadores. En estos sistemas, los datos pueden ser replicados y almacenados en distintas ubicaciones físicas, con el propósito de evitar el problema del punto único de fallo"[30].

En estas redes, la información se distribuye entre todos los nodos que integran la red. Esto permite que los registros se mantengan protegidos de forma segura en cada uno de estos ordenadores. A diferencia de los sistemas centralizados, donde un único servidor conserva la información —con los riesgos inherentes de pérdida o alteración—, en las redes descentralizadas la seguridad se fortalece gracias a esta distribución. “En una red distribuida, es preciso un mecanismo de consenso para que los nodos se pongan de acuerdo sobre el registro de los datos compartidos. Por ello cada una de estas redes tiene su propio protocolo que consiste en las reglas y procedimientos que los nodos deben seguir para compartir y verificar datos.”[31]

En la actualidad, existen múltiples redes descentralizadas basadas en tecnología *blockchain,* como Bitcoin, Ethereum o Solana. Este tipo de redes son particularmente idóneas para el registro seguro de documentos electrónicos, ya que, al no depender de un administrador central, la información almacenada no puede ser manipulada, intervenida ni eliminada.

[29] Momento en que nació la *blockchain* de Bitcoin.
[30] *Idem*.
[31] *Idem.*

b) Redes públicas y privadas

Públicas: También denominadas "no permisionadas", son cadenas de bloques abiertas a cualquier persona que desee participar, permitiendo el registro de transacciones y la participación en los mecanismos de consenso, sin que exista un órgano administrador que las regule. Ejemplos de este tipo de redes son Bitcoin y Ethereum.

La idea primigenia detrás de la creación de *blockchain* fue precisamente la de establecer una red pública y abierta. Bitcoin nació como una respuesta y alternativa a los sistemas centralizados y privados, como las redes bancarias tradicionales. Este tipo de redes, al ser públicas, ofrecen una mayor seguridad frente a la manipulación de la información, dado que están integradas por individuos que no se conocen entre sí ni tienen vínculos, su manipulación resulta prácticamente imposible.

Privadas: Son cadenas de bloques cerradas, en las cuales solo pueden participar determinados integrantes previamente autorizados, quienes detentan el control y la administración de la red.

Este tipo de redes son susceptibles de ser intervenidas o alteradas, al estar bajo la gestión de un grupo cerrado de usuarios que controla los registros.

c) Permisionadas y no permisionadas.

Permisionadas: Este tipo de redes otorgan credenciales o permisos a un grupo específico de personas para que puedan llevar a cabo registros y ejercer control sobre la información.

No permisionadas: En estas redes, cualquier usuario puede integrarse a los mecanismos de consenso sin necesidad de permisos especiales.

Al no requerirse autorizaciones para el acceso, la información registrada en redes no permisionadas es difícil de manipular, lo cual las convierte en plataformas idóneas para el registro de medios electrónicos con valor probatorio en juicios digitales.

Una vez precisados el concepto y los elementos de la tecnología *blockchain,* podemos proceder al análisis de su regulación en el Código Nacional de Procedimientos Civiles y Familiares (CNPCF).

III. La tecnología *blockchain* en el Código Nacional de Procedimientos Civiles y Familiares.

3.1 Justicia digital.

El 7 de junio de 2023 fue publicado en el *Diario Oficial de la Federación* el Código Nacional de Procedimientos Civiles y Familiares (CNPCF), ordenamiento que consagra e institucionaliza el sistema de justicia digital como una alternativa válida al procedimiento judicial de carácter presencial. Asimismo, dicho cuerpo normativo reconoce el uso de tecnologías emergentes, tales como la blockchain, como medios legítimos para el registro de información electrónica, susceptible de ser incorporada al juicio como medio probatorio, con pleno valor jurídico, siempre que se cumplan los requisitos legales establecidos.

En primer término, resulta pertinente destacar que la implementación del sistema de justicia digital fortalece de manera significativa el derecho fundamental de acceso a la justicia, consagrado en el artículo 17 de la Constitución Política de los Estados Unidos Mexicanos. Por una parte, dicho sistema contribuye a la celeridad procesal, al descongestionar la carga de trabajo de los órganos jurisdiccionales; por otra, acerca los servicios jurisdiccionales a los justiciables, quienes pueden comparecer en juicio a través de plataformas electrónicas desde el lugar en el que se encuentren, sin necesidad de desplazarse físicamente al tribunal.

Al respecto, Miguel Carbonell ha señalado que el acceso a la justicia puede verse vulnerado por condiciones geográficas, al sostener que: “El aparato judicial, en general, en buena parte de América Latina, no ha podido tener una presencia

efectiva en la totalidad del territorio de los países, de modo que un primer obstáculo para el acceso a la justicia es simplemente de carácter físico o geográfico."[32]

En el contexto latinoamericano, y particularmente en México, la mayor parte de los órganos jurisdiccionales se ubican en zonas urbanas, lo cual impone una carga desproporcionada a las personas que habitan en zonas rurales o marginadas, quienes deben recorrer largas distancias con altos costos económicos y temporales para ejercer su derecho a la tutela jurisdiccional efectiva. La justicia en línea, en consecuencia, constituye una vía idónea para acercar la función jurisdiccional a las poblaciones alejadas, materializando así el principio de proximidad judicial[33].

Adicionalmente, la justicia digital representa una herramienta de inclusión procesal para personas con discapacidad, quienes enfrentan obstáculos estructurales y de accesibilidad en los espacios físicos de los tribunales, los cuales muchas veces carecen de ajustes razonables, diseño universal, infraestructura accesible y condiciones de integración efectiva, en contravención de lo dispuesto por la Convención sobre los Derechos de las Personas con Discapacidad[34] y la Ley General para la Inclusión de las Personas con Discapacidad[35].

El artículo 2º, fracción XXXV, del CNPCF define al sistema de justicia digital, como:

> Todo dispositivo electrónico, programa de cómputo, aplicación, **herramienta tecnológica** o plataforma electrónica, propiedad del Poder Judicial o de terceros, que sea utilizada para consultar, usar, enviar o llevar a cabo procedimientos en línea, audiencias virtuales, diligencias virtuales, expedientes electrónicos, firmas electrónicas, mensajes de datos,

[32] Carbonell Miguel, *Los Derechos fundamentales en México*, México, Ed. Porrúa, 2024, p.723.
[33] No podemos olvidar que otro gran problema que el Estado debe atacar es que en varias zonas rurales el acceso a internet es limitado.
[34] Firmada por México en el 2007, disponible en *https://www.cndh.org.mx/sites/default/files/documentos/2019-05/Discapacidad-Protocolo-*Facultativo%5B1%5D.pdf, (29 de julio de 2025).
[35] Disponible en *https://www.diputados.gob.mx/LeyesBiblio/pdf/LGIPD.pdf,* (29 de julio de 2025).

documentos electrónicos o digitalizados, promociones electrónicas, salas virtuales y videoconferencias.

A partir de dicha definición, se infiere que el sistema de justicia digital no sólo permite, sino que autoriza expresamente la incorporación de herramientas tecnológicas al proceso judicial. En este contexto, la tecnología *blockchain* se erige como una herramienta idónea para el registro, conservación y verificación de documentos electrónicos, aportando certeza, inmutabilidad, integridad y trazabilidad a los medios probatorios que sean incorporados al juicio.

3.2 La tecnología *blockchain* en el CNPCF

Una de las novedades más destacables que presenta el CNPCF es la inclusión de le tecnología *blockchain* como medio para registrar y conservar información electrónica de manera segura.

La cadena de bloques (*blockchain*) es definida por el CNPCF en el artículo 2º fracción VII:

> **Artículo 2.** Para los efectos de este Código Nacional de Procedimientos Civiles y Familiares, se entenderá por:
> **VII. Cadena de bloques**. Conjunto de tecnologías cuyas características buscan posibilitar la transferencia de valor en entornos digitales a través de métodos de consenso y cifrado. Desde un punto de vista técnico, y atendiendo a sus características, una cadena de bloques es una base de datos, descentralizada y distribuida en una red de computadoras, formada por un conjunto de registros vinculados donde se almacenan transacciones o datos, que han sido diseñados para evitar su modificación o manipulación no autorizada, una vez que un dato ha sido publicado. Una cadena de bloques es pública cuando es abierta, transparente, cualquiera puede unirse, tener acceso a ella, enviar transacciones y participar en el proceso de consenso o validación de datos. Se consideran cadenas de bloques sin

permiso o no permisionadas, ya que no hay restricciones y la participación en ellas no está controlada por un administrador o por un cuerpo central de gobierno.

Dicha definición se alinea con los elementos doctrinales y técnicos expuestos anteriormente, por lo que resulta pertinente desglosar sus componentes fundamentales para una mejor comprensión:

a) **Tecnología de registro digital distribuido**: Permite la inscripción de documentos, activos o información electrónica diversa —como contratos, actas, títulos de crédito, mensajes electrónicos (WhatsApp, correos electrónicos), criptoactivos, tokens no fungibles (NFT), certificados digitales y documentos oficiales— asegurando su integridad y permanencia.

b) **Métodos de consenso y cifrado criptográfico**: Toda transacción o inscripción en la cadena requiere ser validada por una mayoría de nodos mediante mecanismos de consenso (por ejemplo, *proof-of-work* o *proof-of-stake*), y se almacena mediante técnicas de cifrado asimétrico que utilizan claves públicas y privadas, lo cual garantiza confidencialidad, transparencia e inmutabilidad.

c) **Base de datos descentralizada y distribuida**: A diferencia de los sistemas centralizados, la *blockchain* opera sin autoridad jerárquica, pues el control del registro se distribuye entre nodos interconectados que almacenan réplicas completas de la cadena, reduciendo significativamente el riesgo de manipulación o pérdida de la información.

d) **Requisitos probatorios específicos**: El CNPCF únicamente reconoce efectos jurídicos a los registros contenidos en redes *blockchain* que sean públicas, descentralizadas y no permisionadas. Esto implica la exclusión de las cadenas de bloques privadas o permisionadas, por considerarse susceptibles de alteración al estar bajo el control de entidades centralizadas que pueden incidir en la operación de los nodos autorizados, comprometiendo así la autenticidad y fiabilidad de los datos.

En consecuencia, el CNPCF reconoce la cadena de bloques como una herramienta tecnológica idónea y jurídicamente válida dentro del sistema de justicia digital, ya sea empleada por el Poder Judicial o por terceros. Su funcionalidad permite el resguardo seguro e inalterable de mensajes de datos, los cuales —de cumplir con los criterios establecidos en el ordenamiento— podrán ser valorados como prueba plena en juicio.

A continuación, se abordarán los requisitos técnicos y jurídicos necesarios para dotar de valor probatorio a los registros efectuados en tecnología *blockchain.*

3.3 La *blockchain* como medio de prueba.

3.3.1 Requisitos de validez de los mensajes de datos para ser considerados prueba plena.

El CNPCF reconoce a la tecnología *blockchain* pública, descentralizada y no permisionada como una herramienta tecnológica segura de generación y conservación de mensajes de datos. Sin embargo, para que los mensajes de datos registrados en esta tecnología, tengan valor probatorio pleno, es necesario cumplir con los requisitos legales que impone el Código, los cuales analizaremos en este capítulo.

Una de las aportaciones más relevantes del nuevo Código Nacional de Procedimientos Civiles y Familiares (CNPCF) es el reconocimiento expreso del valor probatorio de los mensajes de datos generados y comunicados mediante tecnologías como la cadena de bloques pública y descentralizada. El artículo 348 establece lo siguiente:[36]:

[36] Los requisitos exigidos por el CNPCF son acordes con los requeridos por la NOM 151-2016 Sobre los Requisitos que Deben Observarse para la Conservación de Mensajes de Datos y Digitalización de Documentos, en su apéndice C2, el cual establece:
"1. El mensaje de datos que se envíe deberá mantenerse íntegro, confidencial y disponible desde el momento de su envío y hasta su recepción.
Lo cual se logra con un registro en una cadena de bloques, en donde el mensaje permanece registrado de manera segura.
2. Cuando las disposiciones legales aplicables así lo requieran, las partes deberán garantizar fehacientemente la identidad de las partes en el envío y recepción del mensaje de datos.
Para lo cual se debe utilizar una firma electrónica avanzada.
3. Cuando las disposiciones legales aplicables así lo requieran, deberán incluir el tiempo en que se

> "Artículo 348: "Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos, digitales, en una **cadena de bloques** o en cualquier otra tecnología[37]"

De lo anterior se desprende que el legislador ha incorporado de manera explícita la tecnología *blockchain* como un mecanismo idóneo para la generación y conservación de información electrónica que pueda ser utilizada como medio de prueba dentro de un proceso jurisdiccional.

El artículo 2º, fracción XXV, del mismo ordenamiento, define el mensaje de datos como: "La información generada, enviada, recibida, archivada o comunicada a través de medios de comunicación electrónica, que puede contener documentos electrónicos."

En consecuencia, se entiende por mensaje de datos toda manifestación electrónica de información, sin importar su naturaleza —contractual, probatoria, declarativa, etc.—, siempre que haya sido generada o conservada por medios tecnológicos, como un correo electrónico, una conversación de mensajería instantánea (WhatsApp), un archivo PDF firmado, entre otros.

Ahora bien, la eficacia probatoria de los mensajes de datos estará condicionada a la observancia de los requisitos que dispone el artículo 349 del CNPCF, el cual establece:

envía y recibe el mensaje de datos."
Diario Oficial de la Federación 30 de marzo de 2017, disponible en *https://www.dof.gob.mx/normasOficiales/6499/seeco11_C/seeco11_C.html,* (28 de julio de 2025).

[37] Cualquier otra tecnología podría ser el metaverso. Matthew Ball lo define como "una red masiva e interoperable de mundos virtuales 3D renderizados en tiempo real que pueden ser experimentados de forma sincrónica y persistente por un número efectivamente ilimitado de usuarios con un sentido de presencia individual, y con continuidad de datos, como identidad, historia, derechos, objetos, comunicaciones y pagos." Ball, Matthew. *El metaverso,* Trad. Aurora González Sanz, México, Paidós, 2022, p.55.
El CNPCF la define en el artículo 2º, fracción XXVI:
"Metaverso. Espacio virtual que posibilita la convivencia social en mundos digitales a través de experiencias gráficas inmersivas en tercera dimensión, que suele utilizar tecnologías de realidad virtual, realidad aumentada, realidad mixta o híbrida, tokens y cadena de bloques" …

> Para valorar la fuerza probatoria de la información a que se refiere el artículo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

De esta disposición se derivan tres elementos esenciales para que un mensaje de datos sea considerado como prueba plena:

a) Fiabilidad del método de generación, comunicación, recepción o archivo. Este requisito se satisface mediante el uso de tecnologías que garanticen integridad y trazabilidad. La tecnología *blockchain*, en su versión pública y descentralizada, resulta especialmente idónea, ya que toda transacción se valida por consenso entre nodos y queda registrada mediante funciones hash criptográficas, impidiendo su alteración posterior. Además, puede incorporar sellos de tiempo que acreditan el momento exacto de su creación, conforme a la NOM-151-SCFI-2016.

b) Conservación íntegra y segura del mensaje de datos para su ulterior consulta. El almacenamiento en una cadena de bloques garantiza que la información no pueda ser modificada sin que ello se detecte en la estructura de bloques posteriores, asegurando así la inmutabilidad del registro. El acceso a dicha información se realiza mediante llaves criptográficas públicas y privadas, lo cual garantiza la confidencialidad y control de acceso.

c) Atribución del contenido a la persona obligada. Este requisito se cumple mediante el uso de la firma electrónica avanzada, definida en el artículo 2º, fracción

XX, del CNPCF[38], y regulada por la Ley de Firma Electrónica Avanzada[39]. La firma electrónica avanzada amparada por un certificado digital vigente garantiza no solo la identidad del firmante, sino también la integridad del documento firmado. El artículo 949 del CNPCF reconoce que las actuaciones suscritas con firma electrónica avanzada tienen los mismos efectos jurídicos que aquellas con firma autógrafa:

> **Artículo 949.** Las actuaciones y promociones judiciales contenidas en un mensaje de datos o documento electrónico suscritas con una firma electrónica avanzada amparada por un certificado digital vigente, garantizará la integridad del documento y producirá los mismos efectos que las leyes otorgan a los documentos con firma autógrafa, teniendo el mismo valor probatorio.

Cabe señalar que en México existen prestadores de servicios de certificación autorizados por la Secretaría de Economía[40], quienes emiten los certificados digitales que autentican las firmas electrónicas. Estos certificados, cuando se vinculan al mensaje de datos registrado en una *blockchain* pública, cumplen con los estándares exigidos tanto por la LFEA como por la NOM-151-SCFI-2016.

En ese sentido, la doctrina nacional ha señalado que la aplicación de criptografía asimétrica —*hash*, cifrado, firma electrónica, y sello de tiempo— otorga a los registros electrónicos una robustez técnica que supera ampliamente a los

[38] "Artículo 2º Firma electrónica avanzada. El conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa. La firma electrónica avanzada prevalece frente a la firma electrónica simple, ya que los requisitos de producción de la primera la dotan de más seguridad que la segunda. A pesar de que las autoridades utilicen una terminología distinta para este tipo de firma, si la misma cuenta con los atributos y características señaladas en esta definición, será considerada como firma electrónica avanzada para los efectos de este Código Nacional."
[39] Ley de Firma Electrónica Avanzada, *op, cit.*
[40] Para mayor información visitar: *https://www.gob.mx/se/acciones-y-programas/prestadores-de-servicios-de-certificación*, (10 de junio de 2025).

medios tradicionales. Como apunta el maestro Oliva León[41], la tecnología *blockchain* ofrece garantías de autenticidad e integridad imposibles de replicar en documentos físicos manuscritos.

En consecuencia, cuando un mensaje de datos cumple con los requisitos anteriores, puede equipararse jurídicamente a un documento original. El artículo 350 del CNPCF así lo reconoce:

> **Artículo 350.** Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos, digitales, cuánticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.

El diseño técnico de la cadena de bloques —mediante su estructura encadenada de bloques, cada uno identificado mediante *hash* y con marca de tiempo— permite verificar cualquier intento de alteración, ya que una mínima modificación altera toda la cadena posterior. Esta inmutabilidad es lo que confiere valor de prueba plena, análoga a la documental pública, cuando no existan indicios de vulneración de la red.

No obstante, debe hacerse una advertencia doctrinal. Como señala Pizaña[42], la prueba plena derivada del mensaje de datos registrado en una *blockchain* está condicionada a que no existan elementos fehacientes que desacrediten su integridad o autenticidad. La cadena de bloques garantiza la existencia y

[41] Oliva León, Ricardo. *Transformación Digital y Tecnología de la Justicia. Fintech, Regtech, y Legalteck,* Valencia, *Tirant lo blanch,* 2020, p.477.
[42] Pizaña D, *Blockchain como Prueba Plena*. Código Nacional de Procedimientos Civiles y Familiares (curso en línea), Plataforma *Lawgic,* 2023.

conservación de la información, pero no su veracidad material, la cual deberá ser probada mediante otros medios de prueba, si se cuestiona su contenido.

Por ello, se recomienda el uso de pruebas preconstituidas: mensajes de datos generados de forma anticipada al juicio con los elementos probatorios completos (*blockchain* pública, firma electrónica avanzada, cláusulas de sometimiento a la tecnología, etc.). Dichos documentos electrónicos deben incorporar expresamente:

- La identificación de la plataforma blockchain utilizada (pública y descentralizada[43].
- Las direcciones electrónicas de los firmantes, declaradas bajo su dominio exclusivo,
- El uso de firmas electrónicas avanzadas con certificado digital vigente[44].,
- Y la voluntad expresa de las partes de utilizar dicha tecnología para el almacenamiento y gestión de sus declaraciones.

Cuando estas condiciones se satisfacen, el juzgador podrá valorar el documento electrónico como prueba plena, con la misma fuerza que un instrumento notarial o una documental pública.

3.3.2 Prestadores de servicios digitales.

En el entorno digital, existen prestadores de servicios tecnológicos que ofrecen plataformas mediante las cuales se permite el acceso a redes públicas y descentralizadas de tecnología *blockchain*, con el objeto de realizar registros de mensajes de datos y generar firmas electrónicas confiables. Estas plataformas están diseñadas para cumplir con los requisitos técnicos y legales de inmutabilidad, trazabilidad, atribuibilidad y conservación, establecidos tanto por la Norma Oficial Mexicana NOM-151-SCFI-2016 como por el Código Nacional de Procedimientos Civiles y Familiares (CNPCF). A través de dichos servicios, se obtiene además la

[43] Ejemplo: Trato.
[44] Existen plataformas en donde la comunicación entre las partes se da a través de ellas como intermediarias.

constancia de certificación de datos y firmas electrónicas, en estricto apego a la NOM-151, también conocida como *"time stamp certificate"* [45], expedida por la Secretaría de Economía, la cual actúa como autoridad certificadora de las transacciones registradas en la blockchain[46]

Dicho certificado incluye, entre otros, los siguientes elementos:

- Número de identificación único de la transacción.
- Fecha de expedición del certificado.
- Código hash y root hash correspondientes.
- Identificación de los participantes en la transacción.
- Firma electrónica.
- Datos para la verificación del documento (SHA).

En la práctica procesal, cuando una de las partes ofrece como prueba un documento registrado en *blockchain,* la autoridad judicial somete dicho documento —comúnmente acompañado del certificado de sello de tiempo (*time stamp*)— a un proceso de verificación. Esta verificación puede realizarse mediante el portal electrónico de la Secretaría de Economía, o bien a través de la plataforma específica empleada por las partes para la generación y registro del documento. Con ello, el órgano jurisdiccional corrobora que el mensaje de datos cumple con los requisitos de generación, conservación e integridad establecidos por el CNPCF y la NOM-151, dotándolo así de valor probatorio pleno.

[45] NOM 51, *op.cit.*
[46] El artículo 972 del CNPCF, en su último párrafo establece que:
"El Consejo de la Judicatura respectivo emitirá Lineamientos de Seguridad de la Información, y todos aquellos que considere pertinentes para dotar de seguridad jurídica y tecnológica a los procedimientos en línea.
"Así mismo, el artículo 15 transitorio del CNPCF determina que:
En materia de digitalización de documentos en expedientes judiciales, mientras el Consejo de la Judicatura respectivo no establezca sus propios lineamientos, deberá cumplirse lo que para tal efecto establece la Norma Oficial Mexicana (NOM 51) que señala los requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos".
Al día de hoy, el Consejo de la Judicatura Federal, no ha emitido lineamientos para dar seguridad a la justicia digital, por lo que es aplicable lo prescrito por la NOM 51.

Es relevante precisar que el *hash*, como identificador criptográfico único del documento, queda registrado tanto en la cadena de bloques pública utilizada, como ante la Secretaría de Economía, que funge como autoridad certificadora. Esta doble verificación refuerza la autenticidad e integridad del documento electrónico ofrecido como prueba.

En este sentido, el jurista Bernardo Perera[47] destaca que "la mayoría de las plataformas intermediarias que ofrecen estos servicios emiten diversos certificados que constituyen documentos idóneos para consolidar el medio de prueba". Entre los documentos usualmente expedidos por dichas plataformas se encuentran: el certificado de utilización de la NOM-151, debidamente sellado por la Secretaría de Economía; la representación gráfica del documento; así como el certificado de notarización en *blockchain* del mismo. Tales documentos, en sus formatos originales, constituyen la información digital original, susceptible de ser presentada como prueba plena dentro de un procedimiento judicial.

3.3.3 Forma de presentar las evidencias con *blockchain*: Presentación, autenticación y desahogo de pruebas registradas en la cadena de bloques.

a) Ofrecimiento oportuno de pruebas

Las pruebas documentales que reposan en una cadena de bloques pública y descentralizada deberán ser ofrecidas en los escritos iniciales de demanda, contestación, reconvención o sus respectivas contestaciones, conforme a lo establecido en el artículo 274 del Código Nacional de Procedimientos Civiles y Familiares (CNPCF):

[47] Perera calzada, Bernardo. "Blockchain como prueba plena". Revista Asesores, México, 2025, disponible en disponible *en https://revistaasesores.com.mx/blockchain-como-prueba-plena/* (31 de julio de 2025).

> **Artículo 274.** Las pruebas deberán ofrecerse en los escritos de demanda, contestación a la demanda, en la reconvención, y en el escrito de contestación a la reconvención, así como de las excepciones. En el caso de incidentes, se hará en el escrito que lo promueva y su contestación, si se realiza por escrito o, en el mismo acto, si se realiza oralmente en la audiencia respectiva.

Es jurídicamente recomendable que, al momento de ofrecer este tipo de pruebas tecnológicas, se proponga también el desahogo de una prueba pericial en informática, con especialidad en tecnología *blockchain*, a fin de que el perito correspondiente fundamente ante la autoridad judicial la naturaleza técnica del medio de conservación y las garantías tecnológicas de autenticidad, integridad y no repudio que la cadena de bloques ofrece. Ello resulta indispensable, en tanto que el conocimiento técnico sobre estos sistemas no es de dominio generalizado entre los juzgadores.

b) Autenticación y acreditación de validez

Para lograr la admisión y valoración adecuada de las pruebas electrónicas registradas en *blockchain,* resulta imprescindible demostrar de forma precisa y documentada el método de generación, conservación, autenticación y acceso del mensaje de datos o evidencia digital. Ello incluye, entre otros, los acuses de recibo, sellos de tiempo *(timestamp*), *hash* criptográfico, número de bloque donde se encuentra la transacción, constancia de certificación y claves criptográficas asociadas.

Lo anterior tiene fundamento tanto en el artículo 2, fracción VII del CNPCF como en la NOM-151-SCFI-2016, que exige que los mensajes de datos se generen y conserven mediante métodos técnicamente confiables, inmutables y consultables a posteriori.

En consecuencia, el escrito de demanda o contestación que ofrezca pruebas registradas en *blockchain* deberá contener:

- Identificación clara de la *blockchain* pública y descentralizada utilizada;

- El *hash* correspondiente al mensaje de datos;
- Número de bloque(s) donde se encuentra almacenada la transacción;
- Acuses de creación y sello de tiempo certificado;
- Certificados de conservación;
- Claves asimétricas necesarias para descifrar la información registrada.

Como señala Bueno de Mata, para efectos procesales, la introducción de pruebas derivadas de *blockchain* debe realizarse incorporando: "el soporte electrónico, así como la copia impresa del hash de la transacción, y de los bloques afectados, junto a las claves criptográficas que permitan su descodificación."[48]

De esta forma, se cumple lo dispuesto por el artículo 349 del CNPCF, que establece:

> Para valorar la fuerza probatoria de la información a que se refiere el artículo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

c) Desahogo de la prueba ante el juzgado

Un aspecto igualmente trascendental en el marco probatorio de evidencias tecnológicas, particularmente aquellas asentadas en tecnología *blockchain*, es la necesidad de proporcionar al órgano jurisdiccional los medios idóneos para su consulta, análisis y valoración. Lo anterior se debe a que los tribunales, en muchos casos, no disponen de la infraestructura tecnológica necesaria para el desahogo de este tipo de pruebas digitales.

[48] Bueno de Mata, F, *Aspectos procesales del blockchain: prueba y administración de justicia*, Curso superior en derecho: aspectos jurídicos de los *smart contracts* y *blockchain,* Plataforma Fundación Universidad de Salamanca/Doinglobal (en línea), 2023, p15.

El artículo 335 del Código Nacional de Procedimientos Civiles y Familiares (CNPCF) reconoce como medios probatorios válidos aquellos sustentados en soportes tecnológicos, incluyendo expresamente aquellos derivados de tecnologías emergentes como la *blockchain.* Sin embargo, impone al oferente de la prueba la carga procesal de garantizar los medios técnicos indispensables para su desahogo, apercibiéndolo de que, en caso de incumplimiento, la prueba será desechada:

> **Artículo 335.** Para acreditar hechos o circunstancias que tengan relación con el procedimiento que se ventile, las partes pueden presentar otros medios de prueba que no estén expresamente reconocidos y regulados en el Código Nacional, como son, ejemplificativamente, videos, fotografías, cintas cinematográficas, disquetes o discos compactos, de sistemas computacionales, grabaciones de imágenes y sonidos, así como la información generada o comunicada que conste en medios electrónicos, magnéticos, ópticos, u otros medios de reproducción; o bien, copias digitales, impresiones de documentos electrónicos, simples o al carbón, documentos taquigráficos; así como registros dactiloscópicos, fonográficos y, en general, cualesquiera otros elementos proporcionados por la ciencia **y la tecnología**, que puedan producir convicción en el ánimo de la autoridad jurisdiccional.
>
> Las pruebas ofrecidas que, por su naturaleza, requieran de dispositivos electrónicos para su reproducción o percepción, o de alguna traducción o interpretación técnica, serán admitidas siempre y cuando la autoridad jurisdiccional cuente con ellas, y en caso contrario el oferente proporcione dichas herramientas para su desahogo en la audiencia respectiva, bajo el apercibimiento de dejar de recibir la prueba.
>
> Los registros electrónicos generados y publicados en un expediente electrónico, únicamente podrán ofrecerse precisando la liga respectiva, la parte conducente que se desea aportar como prueba, así como el nombre de las partes, número de expediente, tipo de juicio, juzgado en el que se

tramita o tramitó el procedimiento respectivo, y cualquier otro dato que permita a la autoridad jurisdiccional su localización electrónica.

En todo caso, deberán respetarse los principios de equivalencia funcional o no discriminación y de neutralidad tecnológica de todo documento electrónico, conforme a las reglas de la prueba documental, atendiendo a la naturaleza del mismo.

IV. Otras funciones de la tecnología *blockchain* en los sistemas de administración de justicia.

a) La cadena de bloques como mecanismo de aseguramiento de la información en los juicios en línea conforme al CNPCF.

Una innovación destacada introducida por el CNPCF es la posibilidad otorgada a las partes procesales de optar por la tramitación de juicios íntegramente en línea. Si bien no es objeto del presente ensayo desarrollar un análisis exhaustivo sobre dicha modalidad procedimental, sí resulta relevante resaltar que la tecnología *blockchain* constituye una herramienta idónea para garantizar la seguridad, integridad, trazabilidad y autenticidad del expediente judicial electrónico.

El artículo 965, fracción II del CNPCF establece como obligación institucional que los sistemas de justicia digital cuenten con medidas robustas y confiables de seguridad informática. Este mandato puede materializarse mediante la implementación de una red *blockchain* que registre, de forma inalterable, todas las actuaciones procesales y documentos que integran el expediente. En este sentido, el profesor Bueno señala que la red *blockchain* utilizada debe ser de carácter privado, operada exclusivamente por el Poder Judicial, restringiendo su acceso únicamente a los justiciables legítimamente interesados: “La utilización de la blockchain dentro del marco de la administración de justicia habrá de tener lugar dentro de una plataforma privada de bloques y no pública. Solo los justiciables que

tengan intereses dentro de un determinado proceso, y por lo tanto, estén legitimados, podrán conectarse.” [49]

Esta perspectiva encuentra respaldo normativo en el artículo 972 del CNPCF[50], el cual dispone diversas medidas mínimas de seguridad digital que deben implementarse en los procedimientos judiciales electrónicos, destacando la necesidad de utilizar tecnologías que aseguren la conservación íntegra y segura de los datos procesales. En este contexto, la *blockchain* representa una solución tecnológica idónea dada su capacidad para garantizar la inmutabilidad, trazabilidad y consulta futura de la información, consolidándose como un instrumento jurídico-tecnológico indispensable para la justicia digital en México.

b) Los tribunales arbitrales en línea.

La tecnología *blockchain* no solo ha facilitado el almacenamiento seguro e inmutable de mensajes de datos y expedientes electrónicos, sino que también ha propiciado el surgimiento de tribunales arbitrales digitales. Un ejemplo paradigmático de ello es la plataforma Kleros[51], la cual opera sobre la infraestructura de la *blockchain* de Ethereum. Dicha plataforma permite que un conflicto sea sometido a un mecanismo de resolución en línea ante un conjunto de personas seleccionadas aleatoriamente mediante un protocolo descentralizado, quienes actúan como árbitros del caso en cuestión. La decisión se adopta por mayoría y los árbitros que hayan votado conforme al laudo mayoritario son recompensados mediante tokens de criptomoneda nativa de la plataforma (ETH), bajo un sistema de incentivos automatizado.

[49] Bueno, F. *op, cit* , p.17.
[50] “Art 972. ACCIONES BASICAS DE SEGURIDAD. Son acciones básicas de seguridad que debe adoptar la autoridad jurisdiccional, para darle seguridad al expediente electrónico, así como a los procedimientos en línea, y todos los sistemas de justicia digital:
VIII. Aplicar soluciones o mecanismos tecnológicos que aseguren la conservación, integridad y disponibilidad de todas las resoluciones judiciales e información que contenga el expediente electrónico.”
[51] Disponible en *https://kleros.io/,* (31 de julio de 2025).

Asimismo, la tecnología *blockchain* ha sido incorporada en procedimientos arbitrales donde las partes contratantes, mediante cláusula compromisoria expresa, acuerdan someter cualquier controversia derivada del contrato a un tribunal arbitral digital. Un ejemplo de ello es The Blockchain Arbitration Society (BAS) [52], considerada la primera asociación en ofrecer una jurisdicción completamente criptovirtual. Esta organización pone a disposición de empresas y particulares sus capacidades técnicas y jurídicas para brindar asesoría, formación y supervisión en materia de *blockchain* y activos digitales.

En este sentido, puede observarse que el uso de la cadena de bloques en la administración de justicia se encuentra en una fase incipiente, pero con potencial de expansión significativa. Gradualmente, tanto las personas físicas como morales adoptarán esta tecnología, siendo el derecho positivo el encargado de normar y sistematizar tales prácticas conforme a los principios rectores del debido proceso. No resulta descabellado anticipar una futura regulación del registro público de la propiedad sobre una infraestructura *blockchain,* lo cual transformaría radicalmente el paradigma tradicional del tráfico jurídico inmobiliario.

V. Conclusiones.

El uso de la cadena de bloques apenas comienza, poco a poco, las personas y las empresas empezarán a utilizarla y será el derecho quien recoja y reglamente esta realidad dentro del ordenamiento jurídico.

México ha dado su primer paso, mediante la promulgación del Código Nacional de Procedimientos Civiles y Familiares, en donde no solo la define en su artículo 2º fracción VII, sino que aprovecha las características de seguridad, transparencia, confiabilidad e inmutabilidad de esta tecnología para la generación,

[52] Sánchez, Javier, " El blockchain aterriza en el mundo de las criptomonedas: *La blockchain Aritrarior Society* emite su primer laudo", Plataforma Confilegal, 2021, disponible en *https://confilegal.com/20211124-el-arbitraje-aterriza-en-las-criptomonedas-blockchain-arbitrary-society-emite-su-primer-laudo/*,(28 de julio de 2025).

registro y conservación de mensajes de datos.

Son los beneficios que esta tecnología aporta, los que llevan al legislador a considerar que el mensaje de datos contenido en un *blockchain* pública, descentralizada y no permisionada, hace las veces de documento original, si se cumple con los requisitos de i) fiabilidad del método de generación, comunicación, recepción o archivo, ii) conservación íntegra y segura del mensaje de datos para su ulterior consulta y iii) atribución del contenido a la persona obligada. Lo cual se consigue con una firma electrónica avanzada. Cumplidos estos requisitos el mensaje de datos es considerado como documento original, y tiene valor probatorio pleno en juicio.

Por otra parte, las pruebas registradas en unas cadenas de bloques deben ofrecerse en un juicio en el escrito de demanda o contestación, según sea el caso, siendo indispensable señalar la *blockchain* pública y descentralizada utilizada, el *hash* que contiene la información, los acuses de creación, sellos de tiempo, certificados de conservación y claves asimétricas para la desencriptación; así mismo, las partes deben ofrecer los medios tecnológicos que permitan su desahogo, ya que el juzgado no cuenta con ellos.

La tecnología *blockchain* no solo ha facilitado el almacenamiento seguro e inmutable de mensajes de datos y expedientes electrónicos, sino que también ha propiciado el surgimiento de tribunales arbitrales digitales

En un futuro visualizamos el aumento en el uso de esta tecnología, probablemente, en un par de años, contemos en México con un registro público de la propiedad que se encuentre en una *blockchain* creada para ese efecto, por el momento, podemos ampliar el uso de esta tecnología con las nuevas plataformas de justicia digital como Kleros, o bien los tribunales arbitrales como los ofrecidos por la *Blockchain Arbitration Society* (BAS).

VI. Fuentes consultadas.

Libros y recursos electrónicos.

BALL, Matthew, *El metaverso.* Trad. Aurora González Sanz. México, Paidos, 2022.

BUENO, F, Curso superior en derecho: aspectos jurídicos de los *smart contracts* y blockchain, aspectos procesales del blockchain: prueba y administración de Justicia, (en línea), Universidad de Salamanca, Doinglobal, 2023.

DELGADO, A. *Blockchain*: concepto, funcionamiento y aplicaciones, en Gurrea, A, (eds), Fintech, Regtech y Legaltec, Valencia, Tirant lo blanch, 2020.

GORRIS, C, Tecnología blockchain y contratos inteligentes, inteligencia artificial, Valencia, Tirant lo blanch, 2017.

GONZÁLEZ, A, *Blochchain,* curso superior en derecho: aspectos jurídicos de los *smart contracts* y *blockchain,* Universidad de Salamanca/Doinglobal (en línea), 2023.

MARTÍNEZ, José y COLAMA, Juan Carlos. *How Blockchain and Smart Contracts have Change How We Do Business: Legal Perspective.* En Gurrea, A., (eds), *Blockchain, fintech and law*, Valencia, Tirant lo blanch, 2022.

MEDINA, ZEPEDA, Emmanuel, "Hacia una teoría de la *e justice* o justicia digital: instrucciones para armar", Revista Mexicana de Derecho Constitucional, México, número 46, enero-junio 2022.

MERINO, David, *Introducción al Derecho Tecnológico*, México, Juristech, 2019.

OLIVA LEÓN, Ricardo, *Transformación Digital y Tecnología de la Justicia*, Fintech, regtech, y legaltech, Valencia, Tirant lo blanch, 2020.

PIZAÑA, D, *Blockchain como prueba plena,* Curso sobre el Código Nacional de Procedimientos Civiles y Familiares, Plataforma *Lawgic* México (curso en línea), 2023.

PERERA CALZADA, Bernardo. "*Blockchain* como prueba plena". *Revista Asesores*, México, disponible *en https://revistaasesores.com.mx/blockchain-como-prueba-plena/* (31 de julio de 2025)

RÍOS, Yolanda, *Blockchain*, *smart contracts* y administración de justicia, Plataforma *Blockchain inteligence*, 2021, disponible en: *https://blockchainintelligence.es/wp-content/uploads/2021/02/BLOCKCHAIN-SMART-CONTRACTS-Y-ADMINISTRACION-DE JUSTICIA_YOLANDA-RIOS.* (28 de julio de 2025).

SÁNCHEZ, Javier. " El blockchain aterriza en el mundo de las criptomonedas: La blockchain Aritrarior Society emite su primer laudo", Plataforma Confilegal, 2021, disponible en *https://confilegal.com/20211124-el-arbitraje-aterriza-en-las-criptomonedas-blockchain-arbitrary-society-emite-su-primer-laudo/* (28 de julio de 2025)

SCHWAB, Klaus, "La cuarta revolución industrial", México, *Penguin Random House*, 2017.

WORLD JUSTICE PROJECT, Hallazgos principales del Índice de Estado de Derecho en México 2020-2021: Resultados destacados y tendencias, 2021.

Leyes

Cámara de Diputados, Iniciativa con proyecto de decreto por el que se expide el Código Nacional de Procedimientos Civiles y Familiares, 8 de febrero de 2022.

Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación, 5 de febrero de 2017 (última reforma publicada el 15 de abril de 2025).

Código Nacional de Procedimientos Civiles y Familiares (CNPCF), 07 de junio del 2023, (última reforma publicada el 16 de diciembre de 2024).

Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, Nueva York, 23 de noviembre de 2005, Diario Oficial de la Federación, 14 de junio de 2013.

Convención sobre las personas con discapacidad, Nueva York, 13 de diciembre de 2006, Diario Oficial de la Federación, 12 de mayo 2008.

Ley de Firma Electrónica Avanzada, Diario Oficial de la Federación, 11 de enero de 2012 (última reforma publicada el 11 de marzo de 2024).

Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, Diario Oficial de la Federación, 1 de febrero de 2007 (última reforma publicada el 20 de mayo de 2024.

Ley General para la Inclusión de las Personas con Discapacidad, Diario Oficial de

la Federación de 30 de mayo de 2011, (última reforma publicada el14 de junio de 2024).

NORMA Oficial Mexicana NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos. Diario Oficial de la Federación 30 de marzo de 2017. (Cancela la NOM-151-SCFI-2002).

UNCITRAL, *Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996), con su nuevo artículo 5 bis*, Naciones Unidas, publicación 1999.

Fecha de recepción: 14 de enero de 2025.

Fecha de aprobación: 30 de noviembre de 2025.