Oñati Socio-Legal Series (ISSN: 2079-5971)
Oñati International Institute for the Sociology of Law
Avenida Universidad, 8 – Apdo. 28
20560 Oñati – Gipuzkoa – Spain
Tel. (+34) 943 783064 / opo@iisj.net / https://opo.iisj.net

Anonimato, responsabilidad y NFT: los desafíos jurídicos de las transacciones plenamente *on-chain* en *blockchains* públicas

(Anonymity, responsibility and NFTs: Legal challenges of fully on-chain transactions on public blockchains)

OÑATI SOCIO-LEGAL SERIES VOLUME 16, ISSUE 3 (2026), 1145-1166: FRONTERAS DE EXCEPCIÓN: ENTRE EL CONTROL MIGRATORIO Y LA RESISTENCIA MIGRANTE
DOI LINK: HTTPS://DOI.ORG/10.35295/OSLS.IISL.2588
RECEIVED 21 JANUARY 2026, ACCEPTED 9 FEBRUARY 2026, FIRST-ONLINE PUBLISHED 6 MARCH 2026, VERSION OF RECORD PUBLISHED 1 JUNE 2026

JAVIER MARTÍNEZ BOADA*

Resumen

Los tokens no fungibles (NFT) se basan en la tecnología *blockchain* y en los *smart contracts* para permitir la creación y transmisión de activos digitales. Aunque la mayoría de las transacciones de NFT se realizan a través de *marketplaces* centralizados o semidescentralizados, cada vez son más las operaciones ejecutadas completamente *on-chain* sin que intervengan intermediarios identificables. El anonimato relativo de los usuarios en estos entornos dificulta tanto la identificación de las partes como la aplicación efectiva de normas jurídicas que garanticen la seguridad de las transacciones. En este contexto, el presente artículo examina los principales desafíos legales de las transacciones de NFT en *blockchains* públicas y analiza las tensiones estructurales que surgen entre la descentralización, la transnacionalidad y el anonimato característico de esta tecnología y los marcos jurídicos tradicionales.

Palabras clave

Tokens no fungibles; *blockchain*; *smart contracts*; anonimato; *marketplaces*

Abstract

Non-fungible tokens (NFTs) are based on blockchain technology and smart contracts, enabling the creation and transfer of digital assets. Although most NFT transactions take place through centralized or semi-decentralized marketplaces, an increasing number of operations are executed entirely on-chain without the involvement of identifiable intermediaries. The relative anonymity of users in these environments complicates both the identification of parties and the effective application of legal norms that ensure transactional security. In this context, this article examines the main legal

* Doctor en Derecho, Universidad Camilo José Cela, Madrid, España. Email: javier.martinez6@ucjc.edu ORCID: https://orcid.org/0009-0008-5482-4757

challenges posed by NFT transactions on public blockchains and analyzes the structural tensions arising between the decentralization, transnational nature, and anonymity characteristic of this technology and traditional legal frameworks.

Key words

Non-fungible tokens; blockchain; smart contracts; anonymity; marketplaces

Table of contents

1. Introducción

Nos encontramos inmersos en lo que se ha denominado la Sociedad de la Información, caracterizada por la centralidad del conocimiento y de los flujos digitales en la economía, la cultura y las relaciones sociales. Ante esta situación, la tecnología ha dejado de ser un mero instrumento para convertirse en un elemento decisivo dentro de la vida cotidiana de las personas, generando nuevos modelos de interacción, comunicación y de comercio (Molina Cevallos *et al.* 2025, pág. 3).

La digitalización de activos, información y servicios ha transformado la producción y el consumo de bienes, al tiempo que plantea desafíos inéditos para los sistemas legales tradicionales, de modo que, desde esta perspectiva, los tokens no fungibles, en adelante, NFT, emergen como un ejemplo de cómo la innovación tecnológica redefine la propiedad, el valor y la responsabilidad en la era digital (Alcántara Francia 2025, 286).

Los NFT han surgido como una de las aplicaciones más disruptivas de la *blockchain*, al permitir crear, certificar y transferir activos digitales de manera descentralizada, generando en 2021 más de 22 000 millones de dólares en ventas (Kireyev 2022, 2).

A diferencia de las criptomonedas tradicionales, que son uniformes y fungibles, los NFT representan objetos digitales indivisibles y exclusivos, lo que amplía sus aplicaciones en áreas como el arte digital, los coleccionables, los videojuegos o la propiedad intelectual, al tiempo que plantea desafíos legales inéditos derivados de su naturaleza digital, la pseudonimidad de las transacciones y la ausencia de intermediarios centralizados en ciertos esquemas digitales (Salame Ortiz *et al.* 2025, 166).

Actualmente, puede observarse que la mayoría de las actuaciones comerciales con NFT se efectúan mediante el respaldo de *marketplaces* centralizados o semidescentralizados. Al respecto, conviene destacar prestadores de servicios como OpenSea o Binance, los cuales, actúan como intermediarios y custodios de los tokens y ciertamente aportan seguridad jurídica a las transacciones, pues, a través de sus plataformas, se comercializa con los NFT y después se introducen en una *blockchain*, por lo que todo el proceso esta centralizado y las partes son plenamente identificables (Du *et al.* 2022, 1).

A pesar de ello, en los últimos años se ha observado un creciente número de operaciones que se realizan exclusivamente a través de *blockchains* públicas sin el respaldo de estas plataformas (Madine *et al.* 2022, 94188).

En este contexto, donde los usuarios aprovechan plenamente las propiedades intrínsecas de las *blockchains* públicas, aparece un escenario jurídico altamente complejo, dado que la identificación de las partes, la atribución de responsabilidades, la protección del consumidor y la tutela de los derechos de propiedad intelectual se ven significativamente desafiadas en sistemas sin intermediarios ni autoridades centrales que garantizan el anonimato o seudoanonimato de los participantes y operan bajo un ecosistema sin ningún tipo de fronteras en el que pueden coexistir múltiples marcos regulatorios (Zhuk 2025, 11).

Ante esta situación, el presente trabajo se centra en analizar las dos principales formas con las que se comercia con NFT y analiza los desafíos jurídicos asociados a las transacciones de NFT realizadas íntegramente en *blockchains* públicas, prestando especial atención a la pseudonimidad de los usuarios y la limitación de los mecanismos

legales tradicionales para garantizar responsabilidad y cumplimiento normativo. Así las cosas y, bajo tales premisas, se plantea la pregunta central de investigación: ¿Existen riesgos jurídicos en torno a la comercialización de NFT celebrada exclusivamente dentro de ecosistemas *blockchain* públicos?

Con el fin de dar respuesta a dicha cuestión, el presente estudio empleará una metodología de dogmática jurídica de tipo cualitativo, combinando el análisis de la doctrina y de la regulación vigente con un estudio de los distintos modelos de transacción de NFT. En este sentido, se considerarán primero aquellos modelos que se encuentran respaldados bajo las marketplaces donde las legislaciones suelen ser cumplidas y, posteriormente, se analizará el comercio exclusivo plenamente *on-chain* en *blockchains* públicas, como Ethereum y Solana, cuyo carácter descentralizado, transnacional y pseudónimo parece que puede generar importantes riesgos jurídicos y desafíos regulatorios que requerirán de soluciones.

2. NFT, *blockchain* y *smart contracts*: bases técnicas esenciales

Los NFT constituyen una categoría específica de activos digitales cuya principal característica es la no fungibilidad, esto es, la imposibilidad de ser intercambiados de forma equivalente entre sí. A diferencia de los tokens fungibles, como las criptomonedas, cada NFT posee un identificador único registrado en una *blockchain*, lo que permite distinguirlo de cualquier otro token y atribuirle propiedades singulares. De esta forma, dicha unicidad técnica es la que hace posible que los NFT representen activos digitales únicos, ya sean creados directamente en el entorno digital o se encuentren vinculados a bienes o derechos que existen fuera de él, lo que, como puede verse, hace posible nuevas formas de propiedad y de transmisión de esos activos en el ámbito digital (Gámez Baracaldo y Corredor Higuera 2023, 525).

Los NFT requieren necesariamente de la tecnología *blockchain* y de los *smart contracts* para existir y adquirir pleno sentido jurídico y económico, pues dichos mecanismos hacen posible su creación, unicidad, trazabilidad, transferencia y la ejecución automatizada de derechos, razón por la cual resulta imprescindible, con carácter previo, analizar en qué consiste la tecnología *blockchain* y, en particular, el funcionamiento de los *smart contracts* como una de sus funcionalidades esenciales y como bases técnicas indispensables para la comprensión del fenómeno de los NFT (Guardia 2023, 9).

Desde un punto de vista técnico, los NFT funcionan a partir de reglas informáticas conocidas como estándares de tokens, que se desarrollan sobre *blockchains* capaces de ejecutar *smart contracts*. En este ámbito, Ethereum se ha consolidado como la *blockchain* pública programable más utilizada principalmente a través de estándares como ERC-721 y ERC-1155, los cuales determinan cómo se crean, identifican y transfieren los NFT y permiten su interoperabilidad entre distintas plataformas y aplicaciones descentralizadas (Ma *et al.* 2025, 4888).

Con ello, parte de la información asociada al NFT, como sus identificadores o los enlaces al contenido digital, queda registrada directamente en la *blockchain*, lo que posibilita verificar de forma pública y transparente el historial de titularidad y las transacciones realizadas sobre cada token. Sin embargo, como ya puede preverse, el hecho de que estas operaciones se desarrollen en una *blockchain* pública hace que ya podamos plantearnos dudas relevantes en relación con el efectivo cumplimiento de la normativa jurídica

aplicable, ya que estos entornos suelen desenvolverse al margen de los mecanismos tradicionales de supervisión y control legal.

Como se ha adelantado, la infraestructura que hace posible la existencia y circulación de los NFT es la *blockchain*, la cual no tiene un concepto homogéneo entre la doctrina ni una base legal que la defina (Zīle y Strazdiņa 2018, 13).

Como explican algunos autores, la naturaleza jurídica de esta tecnología puede ser definida desde dos posturas que pueden complementarse. Por una parte, puede ser entendida como una base de datos distribuida, inmutable y sincronizada entre múltiples nodos que elimina la necesidad de una autoridad central de confianza y, por otra, como un software o programa informático capaz de autoejecutar condiciones predefinidas mediante los denominados *smart contracts* (Martínez Boada y Rejas Muslera 2024, 6).

Como puede apreciarse, las *blockchains* empleadas para la comercialización de NFT son aquellas que permiten, de manera simultánea, la programación de acuerdos y el registro de transacciones en su propia cadena, es decir, aquellas en las que convergen ambas funcionalidades. En la práctica, como ya se ha señalado, las más utilizadas son *blockchains* públicas como Ethereum o Solana, en las que cualquier usuario puede participar en la red, verificar transacciones y desplegar *smart contracts* sin necesidad de autorización previa. Si bien esta apertura técnica garantiza elevados niveles de transparencia y seguridad, también introduce relevantes implicaciones jurídicas derivadas tanto de la ausencia de un control centralizado como de la naturaleza pseudónima de los participantes (Lampe 2025, 4).

Junto a ello, conviene tener presente de forma breve algunas de las diferentes características que aporta este tipo de tecnología a los usuarios. Como señalan algunos autores, la *blockchain* es distribuida, autónoma, desintermediada, transnacional, pseudoanómina, segura, rápida (Bedecarratz Scholz 2018, 88) y, además, su información es inmutable (Hofmann *et al.* 2017, 1).

En primer lugar, la distribución constituye una de las bases fundamentales del *blockchain* y a diferencia de los sistemas centralizados tradicionales, esta tecnología funciona mediante una red de nodos interconectados en la que cada participante mantiene una copia completa del libro mayor o registro compartido, lo que significa que no existe un único punto de fallo y que la información no depende de ninguna autoridad central para ser validada, lo que garantiza transparencia y resiliencia frente a errores o manipulaciones.

Por otra parte, el sistema es autónomo porque su funcionamiento se sustenta en protocolos criptográficos y reglas predefinidas mediante algoritmos de consenso, lo que permite que las transacciones se validen de manera automática sin intervención humana directa.

Además, la introducción de los *smart contracts* amplía esta autonomía al posibilitar que los acuerdos programados se ejecuten automáticamente cuando se cumplen determinadas condiciones establecidas en el código, lo cual resulta especialmente relevante para este estudio, dado que estos contratos autoejecutables son la columna vertebral de los NFT y de las operaciones plenamente *on-chain*.

Los usuarios pueden interactuar directamente entre sí sin necesidad de actores centrales de confianza, lo que simplifica las transacciones, reduce costes y aumenta la eficiencia, sin embargo, esta autonomía también trae consigo una significativa incertidumbre jurídica, porque en entornos totalmente *on-chain* no existe ninguna autoridad o intermediario que supervise la operación, que pueda validar la identidad de los participantes o garantizar que se cumplan las condiciones contractuales, de modo que cualquier conflicto, error en la ejecución del *smart contract* o incumplimiento de obligaciones recae directamente sobre los usuarios, complicando enormemente la posibilidad de tutela efectiva de derechos y haciendo que, aunque la transacción sea técnicamente perfecta y ejecutada según el código, desde el punto de vista legal exista un vacío que deja expuestos a los participantes.

Asimismo, el carácter transnacional permite que las transacciones puedan realizarse entre usuarios ubicados en distintos países sin que existan barreras geográficas ni regulatorias, lo que facilita la interoperabilidad internacional y la creación de un mercado digital verdaderamente sin fronteras, pero, al mismo tiempo, genera complejos desafíos en materia de regulación y cumplimiento normativo.

En lo que respecta al seudonimato, las transacciones se registran a través de direcciones de wallet que no necesariamente permiten identificar a los usuarios, lo que protege la privacidad, pero complica de manera significativa la imputación de responsabilidades legales y limita la posibilidad de reclamar en caso de fraude, incumplimiento contractual o vulneración de derechos.

Además, la *blockchain* destaca por su seguridad, garantizada mediante criptografía y validación distribuida que dificulta manipulaciones, y por su velocidad, al automatizar procesos y confirmar transacciones en prácticamente segundos.

Finalmente, la inmutabilidad constituye uno de los sellos distintivos de la *blockchain*, pues, toda vez que una transacción es verificada e incorporada a un bloque, pasa a formar parte permanente del registro y no puede modificarse sin alterar toda la cadena posterior, lo que acarrea indudables problemas jurídicos que requieren solución.

A este estudio, le interesan principalmente el pseudoanonimato, la desintermediación, la transnacionalidad y la inmutabilidad de la información, pues son precisamente estas características las que plantean desafíos jurídicos frente a las normas que conforman el Derecho vigente.

Tal y como se ha dicho, la funcionalidad de los *smart contracts* que permiten las *blockchain* programables es esencial para los NFT, pues estos contratos son programas informáticos autoejecutables que se despliegan en la *blockchain*, ejecutan automáticamente instrucciones codificadas cuando se cumplen ciertas condiciones y regulan aspectos clave como la emisión del token, la transferencia de titularidad, la fijación de condiciones de venta y, en muchos casos, la distribución automática de royalties al creador original en ventas secundarias (Fetsyak 2020, 207).

A primera vista, la automatización de los *smart contracts* parece ofrecer solo ventajas, pero introduce una transformación profunda en la manera en que se conciben las relaciones contractuales, pues, a diferencia de los contratos tradicionales, estos programas no interpretan normas jurídicas ni principios generales, sino que ejecutan de forma estricta el código programado. Esta característica plantea interrogantes relevantes

sobre la formación del consentimiento, la existencia de posibles vicios contractuales, la ocurrencia de incumplimientos y la aplicación de figuras clásicas del Derecho como la buena fe o la fuerza mayor, de modo que, aunque desde un punto de vista técnico el contrato siempre se cumpla, desde la perspectiva jurídica no garantiza que el resultado sea necesariamente conforme a la normativa vigente.

Esta circunstancia plantea interrogantes relevantes en relación con la formación del consentimiento y la posible concurrencia de vicios contractuales. En particular, un error en el código, derivado de una programación defectuosa, de una especificación incompleta o de una discrepancia entre la voluntad real de las partes y su traducción algorítmica, puede dar lugar a resultados jurídicamente no deseados, sin que exista un mecanismo interno que permita su corrección. Desde esta perspectiva, el error deja de ser un problema de interpretación para convertirse en un fallo técnico con efectos jurídicos directos.

Asimismo, la existencia de vulnerabilidades conocidas en el ámbito de los *smart contracts*, como los denominados "reentrancy attacks", pone de manifiesto que la ejecución automática puede verse comprometida por comportamientos estratégicos de terceros que explotan defectos del código. En estos supuestos, aunque el contrato se ejecute conforme a sus instrucciones técnicas, el resultado puede ser contrario a la voluntad originaria de las partes y generar situaciones asimilables a un incumplimiento contractual o a un vicio del consentimiento difícilmente encajable en las categorías clásicas del Derecho privado.

Además, todo ello incide también en la aplicación de figuras tradicionales como la buena fe, la fuerza mayor o la imputación del incumplimiento, ya que el carácter automático e inmutable del código dificulta la adaptación del contrato a circunstancias sobrevenidas o excepcionales. En consecuencia, aunque desde un punto de vista técnico el *smart contract* siempre se ejecute, ello no garantiza que el resultado sea necesariamente conforme a la normativa vigente ni que refleje de manera fiel el equilibrio jurídico propio de un contrato válido y eficaz.

Otro aspecto técnico crucial en los NFT es la distinción entre el almacenamiento *on-chain* y off-chain de la información asociada al token. En algunos casos, el contenido digital al que hace referencia el NFT, como imágenes, vídeos o archivos de audio, no se guarda directamente en la *blockchain*, sino en sistemas externos, como, por ejemplo, dentro de las propias marketplaces, las cuales actúan como custodios del contenido y la *blockchain* se limita a automatizar el proceso, registrar la propiedad, transferencias y autenticidad del NFT (Seol *et al.* 2024, 3927).

Junto a ello, es necesario diferenciar entre modelos de interacción intermediados y no intermediados. Dentro de los modelos intermediados, los usuarios interactúan con los NFT a través de marketplaces que actúan como prestadores de servicios que facilitan interfaces, custodia, identificación y cumplimiento normativo, es decir, son los garantes de que exista una autoridad central que supervise y respalde las transacciones evitando que el proceso sea completamente desintermediado o seudónimo, pues, una vez que se comercia con los NFT en dichas plataformas, la *blockchain* se utiliza posteriormente para registrar de manera automática e inmutable las transacciones y ejecutar los *smart contracts* asociados, garantizando trazabilidad, unicidad del token y la automatización de derechos (Kireyev 2022).

Por otra parte, también existen transacciones completamente *on-chain*, en las que los usuarios interactúan directamente en *blockchain* mediante *smart contracts* desde sus propias wallets sin que intervengan intermediarios identificables (marketplaces). En este sentido, se utiliza la misma infraestructura *blockchain* (Ethereum o Solana) que en los modelos intermediados, pero sin la intervención de dicho intermediario (marketplaces), lo que desintermedia el proceso y hace que entren en juego las características propias de la *blockchain* pública como el pseudoanonimato, las cuales pueden generar riesgos jurídicos importantes (Zarifis y Castro 2022, 11).

Como puede observarse, la combinación de *blockchain* pública, *smart contracts* y NFT sin la intervención de un tercero, como un *marketplace*, genera un ecosistema transnacional, descentralizado y pseudónimo, en el que las transacciones se realizan sin referencia a sujetos concretos, a un territorio específico ni a una autoridad central, lo que plantea desafíos a los criterios tradicionales de aplicación del Derecho, basados en la ubicación de las partes, la jurisdicción y la competencia territorial.

Así las cosas, para profundizar en dichos desafíos, a continuación, estudiaremos los NFT intercambiados a través de marketplaces intermediados y, posteriormente, los transacciones plenamente *on-chain*, de manera que podamos comprender las cuestiones jurídicas que plantea este último modelo.

3. Intercambio de NFT a través de *marketplaces*: encaje y regulación jurídica

El comercio de NFT a través de *marketplaces* centralizados o semidescentralizados representa actualmente la forma predominante con la que se transacciona con ese tipo de fichas. Plataformas como OpenSea, Binance NFT, Rarible o Magic Eden no solo facilitan la creación, exhibición y comercialización de tokens no fungibles, sino que también proporcionan un marco de seguridad jurídica robusto, derivado precisamente de posicionarse como ese intermediario identificable que permite reclamar y aporta seguridad a la transacción. A este respecto, este modelo intermediado combina la necesidad de utilizar la tecnología *blockchain* con el cumplimiento legal, constituyendo un punto de encuentro donde se alinean las exigencias de los usuarios y la normativa vigente (Jiménez Serranía 2022, 11).

En estos marketplaces, los usuarios interactúan a través de interfaces centralizadas que permiten identificar a las partes, verificar la titularidad de los NFT y garantizar que las transacciones se ejecutan conforme a las condiciones establecidas en los *smart contracts* subyacentes, de modo que antes de que un NFT se registre en la *blockchain*, la operación se valida internamente en la plataforma, la cual actúa como intermediario de confianza, asegurando que, en caso de discrepancia, error en el *smart contract* o conflicto entre las partes, exista un mecanismo de supervisión y resolución que respalde la transacción (Ekinci 2023, 5).

Un elemento central de seguridad jurídica en los marketplaces es la implementación de procedimientos de identificación de usuarios y cumplimiento normativo, incluyendo mecanismos de KYC (Know Your Customer) y AML (Anti-Money Laundering), que permiten a las plataformas cumplir con la normativa financiera y de prevención del lavado de dinero, así como con estándares de responsabilidad civil en caso de conflicto, garantizando trazabilidad, acceso a registros de transacciones y la posibilidad de

reclamar derechos conforme a la legislación nacional e internacional (Bello *et al.* 2025, 298).

Por contraparte, y por la relevancia que tiene para este estudio, con viene ir advirtiendo que estas salvaguardas no se van a replicar en las transacciones directamente *on-chain* en *blockchains* públicas, dado que en un entorno completamente descentralizado no existe una autoridad central ni identidades verificables a las que atribuir responsabilidades, lo que genera vacíos legales y complica la aplicación de normas y mecanismos tradicionales de supervisión y control (Dolader Retamal *et al.* 2017, 33).

Junto a todo ello, el encaje jurídico se ve reforzado por la naturaleza híbrida de las operaciones en marketplaces, donde la transacción se inicia y valida dentro de la plataforma y solo se registra en la *blockchain* en el momento final de la transferencia del NFT. Este mecanismo tiene dos ventajas esenciales: por un lado, permite que la plataforma controle y valide que todas las condiciones contractuales se cumplan antes de la inmortalización en la *blockchain* y, por otro, mantiene la eficiencia de la tecnología descentralizada al registrar la propiedad y la transferencia de manera segura e inmutable (Ekinci 2023, 5-7).

Igualmente, desde la perspectiva del Derecho, el modelo de marketplaces ofrece una mayor seguridad jurídica en comparación con las transacciones realizadas directamente *on-chain*, dado que existe una entidad responsable que supervisa las operaciones, lo que disminuye significativamente el riesgo de fraude, errores en la transferencia de tokens o disputas sobre la titularidad. Además, esta supervisión también permite identificar la normativa aplicable en caso de controversias, aspecto especialmente relevante considerando el carácter transnacional de la *blockchain*, o si se cumplen con los requisitos del contrato (consentimiento, objeto y causa), ya que en los marketplaces las partes están identificadas y los acuerdos se expresan primeramente en lenguaje natural y luego se codifican en *smart contracts*, cuestión que no ocurre en dentro de las transacciones directas *on-chain*, donde se codifica directamente en lenguaje de programación y solo se puede interpretar por computadoras (Tan 2024, 8).

Como puede observarse, el comercio de NFT a través de marketplaces centralizados o semidescentralizados constituye un modelo en el que la tecnología *blockchain* y los *smart contracts* se integran eficazmente con el marco jurídico existente, garantizando seguridad, trazabilidad y cumplimiento normativo. En este sentido, la presencia de intermediarios responsables, la identificación de usuarios y la verificación previa de las operaciones permiten que las transacciones se realicen dentro de los parámetros legales y reduciendo riesgos que serían significativos en entornos puramente descentralizados (Bhujel y Rahulamathavan 2022, 9).

Evidentemente, aunque en los marketplaces centralizados se respeten en gran medida los derechos de los participantes en el comercio de NFT, estas plataformas no están exentas de la aparición de controversias que requieran resolución. Precisamente, la posibilidad de identificar a las partes involucradas y de celebrar las operaciones inicialmente off-chain, bajo la supervisión de un prestador de servicios que puede asumir la responsabilidad junto con los usuarios, constituye un elemento fundamental que garantiza la aplicación del Derecho y facilita la tutela efectiva de los derechos de los titulares de NFT.

En este sentido, la seguridad jurídica en el comercio de NFT a través de marketplaces encuentra un respaldo sólido en la jurisprudencia reciente, tanto a nivel nacional como internacional.

Por un lado, en el caso de España puede señalarse la Sentencia del Juzgado de lo Mercantil N.º 9 de Barcelona de 11 de enero de 2024 en el caso *VEGAP v Mango* (SJM B 1/2024 - ECLI:ES: JMB:2024:1), en la que se determinó que la utilización de obras protegidas sin autorización para la creación de NFT constituyó una infracción de los derechos de propiedad intelectual. El tribunal confirmó la obligación de indemnizar a los titulares de derechos y de retirar los tokens del mercado, reconociendo que, aunque los NFT operen en entornos digitales y puedan registrarse en la *blockchain*, las normas de propiedad intelectual siguen siendo plenamente aplicables.

Por otro lado, como se mencionó, la *blockchain* es transnacional al igual que el alcance operativo de las propias marketplaces, por lo que también pueden encontrarse pronunciamientos internacionales. Un ejemplo destacado es el caso *Yuga Labs, Inc. vs Ryder Ripps* (*Yuga Labs, Inc. v Ripps* et al, No. 2:2022cv04355 - Document 452 (C.D. Cal. 2024)), que constituye un referente importante sobre la protección de NFT comercializados mediante sistemas intermediados.

En este litigio, los tribunales de Estados Unidos reconocieron que los NFT pueden considerarse "bienes" protegibles bajo la Ley de Marcas (Lanham Act) y confirmaron que la explotación no autorizada de tokens que reproducen o imitan colecciones registradas constituye una infracción susceptible de reclamación judicial. Aunque parte de la resolución fue devuelta al tribunal inferior para analizar elementos específicos del caso, la decisión del Noveno Circuito reafirma que el Derecho puede aplicarse de manera efectiva incluso en contextos transnacionales, siempre que exista un sistema que permita identificar a las partes involucradas y supervisar la transacción, tal como ocurre en marketplaces centralizados.

De esta forma, al menos en el modelo intermediado por marketplaces, los NFT encajan adecuadamente en los marcos legales actuales, constituyendo una base sólida para el comercio digital seguro. Ahora bien, el escenario cambia radicalmente cuando analizamos las transacciones de NFT que se realizan directamente *on-chain*, es decir, sin la intervención de intermediarios como los marketplaces. En este modelo, los usuarios interactúan directamente con los *smart contracts* desde sus wallets, utilizando la misma infraestructura *blockchain* pública, como, por ejemplo, Ethereum o Solana, pero sin que exista una entidad responsable que supervise, valide o medie las operaciones.

Con todo, el comercio de NFT a través de marketplaces centralizados o semidescentralizados parece aportar seguridad jurídica a las transacciones porque garantiza la identificación de las partes y la supervisión previa de las operaciones antes de su registro en la *blockchain*. Así las cosas, puede comenzar a confirmarse que los marketplaces constituyen un entorno seguro y regulado y que los principales desafíos legales emergen prácticamente cuando se eliminan los intermediarios y las transacciones se realizan de manera plena y directa *on-chain*, como se analizará a continuación.

4. Transacciones de NFT plenamente *on-chain* mediante *blockchain* y *smart contracts*: principales problemas jurídicos

Mientras que el comercio de NFT a través de marketplaces se beneficia de mecanismos de identificación, custodia y control que facilitan la aplicación del Derecho y permiten una supervisión previa de las transacciones, las operaciones plenamente *on-chain* presentan un escenario jurídico considerablemente más complejo, dado que la compraventa y transferencia de tokens se realiza directamente entre las wallets de los participantes mediante *smart contracts* autoejecutables, sin la intervención de plataformas centralizadas ni de terceros identificables; este modelo, si bien maximiza la descentralización y la autonomía tecnológica, introduce importantes desafíos legales que derivan fundamentalmente de la pseudonimidad de los usuarios, la irreversibilidad de las transacciones y la transnacionalidad de las operaciones, factores que complican la imputación de responsabilidades, la aplicación de normas vigentes y la protección efectiva de los derechos de las partes involucradas (Tan 2024, 8).

En primer lugar, la pseudonimidad o el anonimato relativo que caracteriza a las *blockchains* públicas constituye uno de los principales obstáculos para la aplicación efectiva del Derecho, puesto que, a diferencia de los marketplaces, donde los usuarios son previamente identificados mediante procedimientos de KYC y AML, en el modelo plenamente *on-chain* no existen identidades tasadas, lo que dificulta de manera considerable la atribución de responsabilidades frente a casos de fraude, incumplimiento contractual o vulneración de derechos.

Como se ha dicho, para operar con NFT dentro de la *blockchain* pública se elaboran acuerdos denominados *smart contracts* que serán plenamente válidos cuando concurran las circunstancias que todo contrato debe cumplir (consentimiento, objeto y causa) (Fetsyak 2020, 211-212). Ahora bien, si los usuarios actúan dentro de un entorno público y directamente *on-chain* resulta extremadamente difícil acreditar la concurrencia de un consentimiento informado y válido, ya que las direcciones de las wallets no contienen, por sí mismas, datos que permitan vincular la voluntad contractual a una persona física identificable; ni siquiera existe certeza de que detrás de una dirección no se encuentre un menor de edad, una persona incapacitada o alguien actuando sin capacidad legal para contratar (Martínez Boada 2024, 21).

Junto a todo ello, debemos tener presente que en un entorno *blockchain* en el que se celebran acuerdos automáticos escritos en lenguaje de programación únicamente interpretables por computadora difícilmente podremos contrastar que el consentimiento y el objeto son válidos conforme a Derecho. Como se vio, en las marketplaces se realiza un acuerdo en lenguaje natural entendible por humanos, para, después, ser automatizado en la *blockchain* mediante un *smart contract*.

En el caso de los negocios plenamente celebrados en *blockchain*, los acuerdos se encuentran directamente codificados y programados en la cadena, lo que hace que únicamente se presenten acuerdos escritos en lenguaje de programación y las partes no entiendan que contiene verdaderamente el contrato. Además, normalmente los usuarios no se encuentran familiarizados con la codificación de estos acuerdos, lo que hace que necesiten acudir a un tercero que redacte y programe el contrato en la cadena.

Ahora bien, el desarrollador o creador del *smart contract* también opera bajo un seudónimo o de manera anónima, lo que imposibilita cualquier reclamación directa frente a posibles fallos en el código, errores en la ejecución o vulneraciones de derechos derivados del contrato, generando un vacío de responsabilidad que, en entornos plenamente *on-chain*, recae directamente sobre los usuarios y limita las posibilidades de tutela efectiva de sus derechos

Junto a la imposibilidad de identificar a los usuarios dentro del los entornos públicos aparece la transnacionalidad que caracteriza a este tipo de sistemas. Como se dijo, *blockchain* no tiene fronteras geográficas, por lo que los usuarios que operan dentro de estos ecosistemas pueden actuar desde cualquier punto del planeta con tan solo tener conexión a internet y un dispositivo informático (Martínez Boada 2025, 1237).

En el ámbito de la Unión Europea, el Reglamento (UE) 2023/1114, relativo a los mercados de criptoactivos (MiCA), constituye un primer intento de ofrecer un marco normativo armonizado frente a estos desafíos. No obstante, su impacto en relación con los NFT resulta limitado y matizado. Si bien el Reglamento excluye, con carácter general, los criptoactivos que sean únicos y no fungibles, prevé expresamente que determinados NFT puedan quedar sujetos a su ámbito de aplicación cuando, por su estructura o forma de emisión, presenten características asimilables a criptoactivos fungibles o se comercialicen de manera masiva.

A partir de 2024, la aplicación de MiCA introduce así un enfoque funcional que atiende más a la realidad económica del criptoactivo que a su denominación formal como NFT, de tal forma que evite el uso instrumental de la etiqueta de "no fungible" para eludir obligaciones regulatorias, pero al mismo tiempo pone de relieve las tensiones persistentes entre un marco jurídico territorial y una tecnología esencialmente transnacional. En consecuencia, aunque MiCA supone un avance significativo en la reducción de la fragmentación normativa dentro de la Unión Europea, no elimina por completo los problemas derivados de la operativa global de los NFT y de los entornos *blockchain*, que continúan planteando importantes retos en términos de supervisión, cumplimiento normativo y protección jurídica de los usuarios.

Aunque el comercio de NFT puede considerarse, desde una perspectiva formal, un tipo de comercio electrónico, la aplicación efectiva de la normativa vigente se ve profundamente limitada en el contexto de transacciones plenamente *on-chain*. A este respecto, la Ley 34/2002, de Servicios de la Sociedad de la Información y Comercio Electrónico, en adelante, LSSICE, establece en sus artículos 2, 10, 21 y 22 diferentes obligaciones claras para los prestadores de servicios digitales como la obligación de proporcionar información completa sobre la identidad del proveedor, los datos de contacto y condiciones de la operación. En el caso de marketplaces intermediados, estas obligaciones se cumplen mediante procedimientos de registro, verificación de identidad y custodia de NFT, lo que garantiza la transparencia de la transacción y la posibilidad de reclamar derechos ante incumplimientos o conductas ilícitas, sin embargo, en un entorno plenamente *on-chain*, donde las transacciones se realizan directamente entre wallets pseudónimas y en un sistema desintermediado en el que no existe autoridad central, no existe un prestador identificado ni un destinatario claramente determinable, lo que impide dar cumplimiento a los requisitos legales de información y protección del consumidor establecidos en la LSSICE.

Además, la problemática se agrava al considerar la dimensión transnacional de la *blockchain* y las normas de jurisdicción internacional. Como se ha dicho, nos encontramos ante relaciones de comercio electrónico, por ejemplo, B2C, en las que, en caso de controversia, deberán aplicarse normativas como el Reglamento (UE) 1215/2012, Bruselas I bis o el Convenio de Lugano II, en los que se establecen criterios precisos para determinar la competencia judicial y la validez de sentencias en casos transfronterizos normalmente basados en el domicilio del demandado (arts. 4 y 7 de Bruselas I bis; arts. 2 y 5 de Lugano II) (Calvo Caravaca 2009, 582).

Cuando la transacción se realiza plenamente en *blockchain*, sin la intervención de una *marketplace*, la pseudonimidad de las wallets impide identificar el domicilio de las partes, lo que convierte prácticamente en imposible determinar un foro competente para dirimir conflictos. De esta forma, nos encontramos ante una situación que genera un vacío legal que limita la eficacia de la tutela judicial y la protección de derechos, incluso cuando la transacción sea equivalente a un contrato electrónico (Martínez Boada 2024, 21).

Junto a ello, los problemas jurídicos en transacciones plenamente *on-chain* también se extienden a la propiedad intelectual y los derechos de autor, dado que los NFT pueden ser creados, transferidos o modificados sin supervisión, lo que incrementa significativamente el riesgo de infracción de derechos de terceros y limita la capacidad de prevenir la comercialización de contenidos ilícitos o no autorizados. Además, de manera análoga, el cumplimiento de obligaciones contractuales, como el pago de royalties o la ejecución de condiciones de uso, depende exclusivamente del código del *smart contract*, de modo que cualquier error o vulnerabilidad en su programación puede derivar en conflictos complejos de remediar jurídicamente.

Por otra parte, otro aspecto que complica la aplicación del Derecho en transacciones plenamente *on-chain* es la diversidad normativa existente entre distintos países, pues cada jurisdicción contempla reglas específicas en materia de contratos, propiedad intelectual, consumo y protección financiera.

Esta heterogeneidad impide determinar de manera clara cuál normativa resultaría aplicable a una transacción determinada, especialmente considerando que la *blockchain* es transnacional y que los participantes pueden residir en distintos territorios. En consecuencia, las obligaciones legales y los mecanismos de protección de derechos varían significativamente según el marco regulatorio de cada país, generando incertidumbre jurídica y dificultando la posibilidad de reclamar, supervisar o remediar cualquier conflicto que surja dentro de un ecosistema descentralizado y sin intermediarios.

Igualmente, la ausencia de intermediarios responsables en los entornos plenamente *on-chain* plantea importantes retos en materia de protección del consumidor y prevención de delitos económicos, como el lavado de dinero o la financiación ilícita, dado que las transacciones se realizan directamente entre wallets pseudónimas sin ningún tipo de control o supervisión.

Además, en lo que concierne a los consumidores, es necesario tener en cuenta que nos encontramos ante un entorno inmutable, en el que la información registrada en la *blockchain* no puede ser eliminada ni modificada y los acuerdos programados en los *smart contracts* se ejecutan automáticamente sin posibilidad de revocación. Esta característica

técnica entra en conflicto con derechos reconocidos en la legislación española y europea, como el derecho de desistimiento previsto en el artículo 102 del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios, ya que, una vez ejecutada la operación *on-chain*, resulta imposible revertir la compraventa o anular el contrato.

De manera similar, ciertos derechos de protección de datos, como la rectificación, supresión o limitación del tratamiento de información personal, establecidos en el Reglamento General de Protección de Datos (RGPD, 2016/679) y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales, no pueden aplicarse plenamente, dado que la naturaleza inmutable de la *blockchain* impide eliminar o modificar registros que contengan datos personales.

En un entorno descentralizado y pseudónimo, garantizar seguridad jurídica frente a estos riesgos resulta extremadamente complejo, ya que no existen intermediarios responsables que puedan ser obligados a responder ni identidades verificables a las que imputar responsabilidades, de este modo, cualquier fraude, manipulación de precios o estafa como "exit scam" queda prácticamente fuera del alcance de la justicia ordinaria, obligando a depender de mecanismos alternativos como arbitrajes descentralizados, seguros externos o protocolos de reputación, los cuales, aunque pueden ofrecer cierto grado de protección, no reemplazan la certeza y supervisión legal que proporcionan los marketplaces centralizados y los tribunales ordinarios (Zarifis y Castro 2022, 4).

Como se vio, en las transacciones realizadas bajo una *marketplace* en la que se conocen las identidades de los usuarios no hay problema para poder solucionar las controversias ante la justicia ordinaria. Las complicaciones surgen, sin embargo, cuando las actividades se desarrollan plenamente dentro de una *blockchain* pública, en la que los participantes no están debidamente identificados y no existe una autoridad central que supervise o pueda ser responsabilizada.

Supongamos que surge un conflicto. En estos sistemas, la resolución depende de sistemas de arbitraje descentralizados como Kleros, donde los árbitros son anónimos, seleccionados mediante incentivos criptográficos y operan exclusivamente sobre la base del código de los *smart contracts*. Como pude verse, esta situación plantea múltiples retos, pues los árbitros pueden carecer de conocimientos legales especializados, sus decisiones no pueden ser impugnadas ni reclamadas y los laudos se ejecutan en código dentro de la *blockchain*, lo que los hace prácticamente incomprensibles para los humanos. Además, aunque teóricamente estos laudos podrían reconocerse bajo convenciones internacionales como la de Nueva York, la falta de identificación y supervisión de los participantes genera importantes vacíos de legitimidad, control y protección efectiva de derechos, aumentando la incertidumbre jurídica en las transacciones efectuadas plenamente *on-chain* (Yépez Idrovo *et al.* 2020, 16).

En el arbitraje convencional, regulado y reconocido internacionalmente a través de instrumentos como la Convención de Nueva York de 1958, la validez y ejecutabilidad del laudo descansan en elementos esenciales como la identificación de las partes y de los árbitros, la posibilidad de control judicial limitado, el respeto al debido proceso y la existencia de una sede arbitral claramente determinada. Estos elementos permiten que los laudos arbitrales puedan ser reconocidos y ejecutados por los tribunales estatales, al

tiempo que ofrecen garantías mínimas de legitimidad, imparcialidad y protección de derechos.

Por el contrario, en los sistemas de arbitraje descentralizado, la ausencia de una sede física, la anonimidad de los árbitros y su eventual falta de formación jurídica especializada dificultan gravemente la aplicación de los estándares exigidos por la Convención de Nueva York. En particular, resulta problemático verificar el respeto al derecho de defensa, la independencia del órgano decisor o incluso la existencia de un verdadero acuerdo arbitral en los términos clásicos del Derecho. Además, las decisiones adoptadas en estos sistemas no suelen ser susceptibles de impugnación o revisión, y su ejecución se produce automáticamente mediante código en la *blockchain*, sin intervención de autoridades judiciales (Pérez Campillo 2025, 6-7).

Si bien, desde un punto de vista teórico, podría sostenerse que determinados laudos *on-chain* podrían aspirar a un reconocimiento internacional, en la práctica la falta de identificación de los árbitros y de las partes, así como la inexistencia de mecanismos de supervisión externa, genera importantes déficits de legitimidad y control. En consecuencia, el arbitraje descentralizado plantea una ruptura con los presupuestos fundamentales del arbitraje tradicional, incrementando la incertidumbre jurídica y poniendo en cuestión la compatibilidad de estos mecanismos con los marcos internacionales de protección efectiva de derechos en las transacciones desarrolladas íntegramente sobre *blockchain*.

Junto a todo ello, hay que tener presente que las nuevas tecnologías se encuentran en constante desarrollo y que el Derecho también evoluciona para adaptarse a esta realidad, de manera que un desafío adicional en las transacciones plenamente *on-chain* radica en el riesgo regulatorio futuro, que surge de la naturaleza dinámica y aún incipiente del marco legal aplicable a los NFT y demás activos digitales, ya que la legislación sobre NFT y activos digitales se encuentra en constante evolución, generando una gran incertidumbre sobre las obligaciones legales presentes y futuras de los participantes.

Como se ha visto, a diferencia de los marketplaces intermediados donde la plataforma puede ajustar sus procedimientos internos a los cambios regulatorios o garantizar que las operaciones cumplan con las normativas emergentes, en la *blockchain* pública los usuarios carecen de cualquier autoridad que vele por la seguridad de los procesos y transacciones efectuados en el sistema.

5. Conclusiones

En conclusión, el análisis realizado evidencia que la seguridad jurídica en el comercio de NFT depende en gran medida del modelo de transacción, siendo los marketplaces centralizados o semidescentralizados los entornos donde se puede garantizar un mayor cumplimiento normativo, tanto nacional como internacional, ya que estos prestadores de servicios actúan como intermediarios responsables, verificando la identidad de los usuarios mediante procedimientos de KYC y AML, custodiando los tokens, supervisando la ejecución de los contratos y asegurando que las partes puedan reclamar ante tribunales o mecanismos legales existentes en caso de conflicto.

Este modelo intermediado permite expresar los acuerdos en lenguaje natural, entendible por las partes, antes de codificarlos en *smart contracts*, garantizando así los requisitos

esenciales del contrato como consentimiento, objeto y causa, y permite la aplicación efectiva de derechos de propiedad intelectual, protección del consumidor y normativa sobre comercio electrónico como la LSSICE, reduciendo significativamente los riesgos de fraude, errores en las transacciones o incumplimiento contractual, y ofreciendo a los usuarios un marco de confianza y previsibilidad jurídica.

La jurisprudencia reciente confirma la eficacia de este modelo, como se observa en la Sentencia del Juzgado de lo Mercantil N.º 9 de Barcelona, *VEGAP v Mango* (SJM B 1/2024), donde se reconoció la obligación de indemnizar a los titulares de derechos por la creación de NFT sin autorización, y en el caso internacional *Yuga Labs, Inc. vs Ryder Ripps* (No. 2:2022cv04355), donde se reafirmó que los NFT pueden ser considerados bienes protegibles bajo la Ley de Marcas, demostrando que, siempre que exista un sistema que identifique a las partes y supervise las transacciones, el Derecho puede aplicarse incluso en contextos transnacionales.

No obstante, la situación cambia radicalmente cuando las transacciones se realizan de manera plenamente *on-chain*, sin intermediarios, pues la pseudonimidad de las wallets, la irreversibilidad de las operaciones y la transnacionalidad del sistema generan desafíos jurídicos relevantes, dado que se dificulta verificar la capacidad legal de los usuarios, la autenticidad del consentimiento y la validez de los acuerdos, especialmente si detrás de una dirección se encuentra un menor, una persona incapaz o alguien actuando sin capacidad para contratar.

El uso exclusivo de *smart contracts* automatizados, aunque garantiza la ejecución técnica de los acuerdos, no sustituye la interpretación legal ni la supervisión humana, de modo que errores de programación, vulnerabilidades del código o diseños contractuales inadecuados pueden generar conflictos de difícil resolución, y la ausencia de intermediarios responsables deja a los participantes expuestos a riesgos que no podrían ser abordados por los tribunales o mecanismos tradicionales de arbitraje, aumentando la incertidumbre jurídica y generando vacíos legales.

La transnacionalidad añade otra capa de complejidad, ya que no existen fronteras físicas ni domicilios fijos, complicando la determinación de foros competentes para dirimir controversias, lo que limita la eficacia de la tutela judicial y la posibilidad de reclamar derechos, especialmente en el marco de reglamentos como Bruselas I bis o el Convenio de Lugano II, que requieren identificar el domicilio de las partes para establecer competencia judicial y validez de sentencias, una exigencia imposible de cumplir en entornos totalmente pseudónimos.

Estos problemas se extienden a la propiedad intelectual y a la protección del consumidor, dado que los NFT pueden crearse, transferirse o modificarse sin supervisión, aumentando el riesgo de infracción de derechos, y cualquier error en la ejecución automática de royalties o condiciones de uso depende del código, sin posibilidad de intervención humana, lo que se agrava por la inmutabilidad de la *blockchain*, que impide revocar transacciones o ajustar acuerdos, entrando en conflicto con derechos reconocidos en la legislación española y europea, como el derecho de desistimiento y el RGPD.

La diversidad normativa entre jurisdicciones añade incertidumbre adicional, ya que cada país contempla reglas distintas sobre contratos, consumo, propiedad intelectual y

regulación financiera, dificultando determinar qué normativa resulta aplicable y exponiendo a los usuarios plenamente *on-chain* a sanciones futuras, especialmente en un contexto donde la regulación sobre NFT y activos digitales está en constante evolución, sin mecanismos proactivos de cumplimiento que protejan a los participantes como ocurre en los marketplaces.

En este contexto, la resolución de conflictos se ve limitada y recurre, en muchos casos, a sistemas de arbitraje descentralizados como Kleros, donde los árbitros son anónimos, seleccionados mediante incentivos criptográficos y operan únicamente sobre la base del código del *smart contract*, lo que reduce la legitimidad, la posibilidad de impugnación y la comprensión de los laudos, dejando a los participantes sin mecanismos efectivos de protección y aumentando la incertidumbre sobre la aplicación de derechos.

Frente a estos desafíos, algunos autores proponen la incorporación de identidades cifradas dentro de las *blockchains* públicas, combinadas con protocolos de reputación verificables, arbitrajes híbridos y mecanismos que vinculen de manera segura los seudónimos a identidades legales, buscando mantener la autonomía tecnológica y la pseudonimidad de los participantes, al tiempo que permiten la aplicación de derechos, la asignación de responsabilidades y la protección efectiva en caso de conflictos, constituyendo una posible solución a los vacíos legales actuales (Martínez Boada 2024, 1-10).En definitiva, este estudio muestra que, mientras los marketplaces ofrecen seguridad jurídica, trazabilidad y supervisión, las transacciones plenamente *on-chain* generan un ecosistema de alto riesgo legal, caracterizado por pseudonimidad, irreversibilidad, transnacionalidad y ausencia de intermediarios responsables, factores que dificultan la aplicación del Derecho, la tutela de derechos y el cumplimiento contractual, dejando a los usuarios expuestos a riesgos que requieren de soluciones innovadoras y adaptadas a la naturaleza descentralizada de la tecnología *blockchain*.

Por todo ello, cualquier desarrollo futuro de la regulación de NFT y de las transacciones en *blockchains* públicas debería enfocarse en mecanismos que combinen la descentralización y la privacidad con seguridad jurídica, supervisión y responsabilidad, explorando alternativas como la identidad cifrada, arbitraje híbrido y protocolos de reputación, de manera que se permita un desarrollo sostenible de la economía digital, equilibrando innovación tecnológica con protección efectiva de los participantes, garantizando certeza jurídica y fomentando la confianza en estos ecosistemas, permitiendo que los NFT puedan circular de forma segura sin renunciar a las ventajas que ofrece la *blockchain*.

Referencias

Alcántara Francia, O. A., 2025. NFTs y derechos de autor: Navegando la frontera digital de la propiedad intelectual. *Revista de Actualidad Mercantil* [en línea], (9), 285-308. Disponible en: https://revistas.pucp.edu.pe/index.php/actualidadmercantil/article/view/30923

Bedecarratz Scholz, F., 2018. Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal. *Revista Chilena de Derecho y Tecnología* [en línea], *7*(1), 79-105. Disponible en: https://doi.org/10.5354/0719-2584.2018.48515

Bello, A., *et al*., 2025. Enhancing Know Your Customer (KYC) and Anti-Money Laundering (AML) compliance using *blockchain*: A business analysis approach. *Iconic Research and Engineering Journals*, *8*(9), 297-305.

Bhujel, S., y Rahulamathavan, Y., 2022. A Survey: Security, Transparency, and Scalability Issues of NFT's and Its Marketplaces. *Sensors* [en línea], *22*(22), 8833, 1-29. Disponible en: https://doi.org/10.3390/s22228833

Calvo Caravaca, A. L., 2009. El Reglamento Roma I sobre la Ley aplicable a las obligaciones contractuales: Cuestiones escogidas. *Cuadernos de Derecho Transnacional*, *1*(2), 52-133.

Dolader Retamal, C., Bel Roig, J., y Muñoz Tapia, J. L., 2017. La *blockchain*: fundamentos, aplicaciones y relación con otras tecnologías disruptivas. *Economía industrial*, 405, 33-40.

Du, L., Kim, M., y Lee, J., 2022. The Art NFT and Their Marketplaces. arXiv preprint *arXiv:2210.14942* [en línea], 1-6. Disponible en: https://doi.org/10.48550/arXiv.2210.14942

Ekinci, Z., 2023. Non-fungible tokens and select art law considerations. *Arts* [en línea], *12*(5), 1-19. Disponible en: https://doi.org/10.3390/arts12050192

Fetsyak, I., 2020. Contratos inteligentes: análisis jurídico desde el marco legal español. *Revista electrónica de Derecho de la Universidad de La Rioja, REDUR* [en línea], (18), 197-236. Disponible en: https://doi.org/10.18172/redur.4898

Gámez Baracaldo, M. C., y Corredor Higuera, J. A., 2023. NFTs (token no fungibles) y sus implicaciones en el mercado de valores. *Derecho PUCP: Revista de la Facultad de Derecho* [en línea], (90), 523-564. Disponible en: https://doi.org/10.18800/derechopucp.202301.015

Guardia, C., 2023. Los derechos de autor en la relación que subyace a los tokens criptográficos no fungibles. *Revista Iberoamericana de la Propiedad Intelectual* [en línea], 19, 7-36. Disponible en: https://doi.org/10.26422/RIPI.2023.1900.gua

Hofmann, F., *et al*., 2017. The immutability concept of *blockchains* and benefits of early standardization. *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society* [en línea], 1-8. Disponible en: https://doi.org/10.23919/ITU-WT.2017.8247004

Jiménez Serranía, V., 2022. Metaverso(s): nuevos retos para las industrias culturales (Especial referencia a los NFTs). *En:* F. Bueno de Mata y I. González Pulido, eds., *Fodertics XI: Derecho, entornos virtuales y tecnologías emergentes*. Granada: Comares, 211-234.

Kireyev, P., 2022. *NFT marketplace design and market intelligence. Kireyev, Pavel, NFT Marketplace Design and Market Intelligence (January 6, 2022). INSEAD Working Paper No. 2022/03/MKT* [en línea], 1-33. Disponible en: https://doi.org/10.2139/ssrn.4002303

Lampe, M., 2025. *A look into adopting NFT technology for medical use in America* [en línea]. 20 de marzo. Disponible en: https://doi.org/10.2139/ssrn.5187742

Ma, Z., *et al*., 2025. Uncovering NFT domain-specific defects on *smart contract* bytecode. *IEEE Transactions on Dependable and Secure Computing* [en línea], 4877-4895. Disponible en: https://doi.org/10.1109/TDSC.2025.3556285

Madine, M., *et al*., 2022. *Blockchain* and NFTs for time-bound access and monetization of private data. *IEEE Access* [en línea], *10*, 94186-94202. Disponible en: https://doi.org/10.1109/ACCESS.2022.3204274

Martínez Boada, J., 2024. Cuestiones jurídicas generadas por los *smart contracts* en el comercio electrónico B2C: foro, jurisdicción aplicable y derecho de desistimiento dentro del ordenamiento jurídico español. *Revista de Derecho (Universidad Católica Dámaso A. Larrañaga, Facultad de Derecho*) [en línea], (30), 1-29. Disponible en: https://doi.org/10.22235/rd30.3919

Martínez Boada, J., 2025. Transformación digital del transporte marítimo: *Blockchain* para la ventanilla única europea. *Cuadernos de Derecho Transnacional* [en línea], *17*(1), 1234-1244. Disponible en: https://doi.org/10.20318/cdt.2025.9365

Martínez Boada, J., 2026. Identidad cifrada con desencriptación judicial: una solución jurídica para la responsabilidad en entornos *blockchain*. *IDP. Revista de Internet, Derecho y Política* [en línea], (44), 1-10. Disponible en: http://dx.doi.org/10.7238/idp.v0i44.9800435

Martínez Boada, J., y Rejas Muslera, R. J., 2024. La protección jurídica de *blockchain*: un análisis desde su funcionalidad y naturaleza jurídica según el ordenamiento jurídico español. *Revista Chilena de Derecho y Tecnología* [en línea], *13*, 1-19. Disponible en: https://doi.org/10.5354/0719-2584.2024.73869

Molina Cevallos, B. K., Ponce Orellana, C. F., y Espinoza Suárez, J. A., 2025. Plataformas digitales frente a la publicidad falsa y *fake news*. Enfoque jurídico. *Revista Social Fronteriza* [en línea], *5*(4), e-831, 1-16. Disponible en: https://doi.org/10.59814/resofro.2025.5(4)831

Pérez Campillo, L. 2025. Implementación de *blockchain* en el sistema judicial público y en los ADR. *IDP. Revista de Internet, Derecho y Política* [en línea], (42), 1-12. Disponible en: https://orcid.org/0000-0002-8047-0293

Salame Ortiz, M. A., Cepeda Luna, C. D., y Granja Zurita, D. F., 2025. Configuración jurídica de los activos digitales y su incorporación en el régimen patrimonial contemporáneo. *Revista UGC* [en línea], *3*(S3), 165-172. Disponible en: https://universidadugc.edu.mx/ojs/index.php/rugc/article/view/238

Seol, J., *et al*., 2024. A non-fungible token (NFT) chain model and performance study. *Cluster Computing* [en línea], *27*(4), 3927-3944. Disponible en: https://doi.org/10.1007/s10586-023-04188-3

Tan, C., 2024. Rights in NFTs and the flourishing of NFT marketplaces. *International Journal of Law and Information Technology* [en línea], *32*, eaae018, 1-17. Disponible en: https://doi.org/10.1093/ijlit/eaae018

Yépez Idrovo, M. V, Vela Sevilla, M. P., y Alegría Haro Aillón, B., 2020. *Smart contracts* y el arbitraje: hacia un modelo de justicia deslocalizado. *SFQ Law Review* [en línea], *7*(1), 1-28. Disponible en: https://doi.org/10.18272/ulr.v7i1.1698

Zarifis, A., y Castro, L., 2022. The NFT purchasing process and the challenges to trust at each stage. *Sustainability* [en línea], *14*(24), 1-13. Disponible en: https://doi.org/10.3390/su142416482

Zhuk, A., 2025. Beyond the *blockchain* hype: addressing legal and regulatory challenges. *SN Social Sciences* [en línea], *5*(2), 11. Disponible en: https://doi.org/10.1007/s43545-024-01044-y

Zīle, K., y Strazdiņa, R., 2018. *Blockchain* use cases and their feasibility. *Applied Computer Systems* [en línea], *23*(1), 12-20. Disponible en: https://doi.org/10.2478/acss-2018-0002

Legislación

Código Civil Español. Arts. 1261 y siguientes sobre contrato, consentimiento, objeto y causa [en línea]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1889-4763

Consejo de Europa, 2007, 30 de octubre. Convenio de Lugano II sobre competencia judicial y reconocimiento y ejecución de resoluciones judiciales en materia civil y mercantil. *DOUE* [en línea], L 339. Disponible en: http://data.europa.eu/eli/convention/2007/712/oj

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico (LSSICE). *BOE* [en línea], 166. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *BOE* [en línea], 294. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

Parlamento Europeo y Consejo de la Unión Europea, 2023. Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos, y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937. *DOUE* [en línea], L 150, 40-205. Disponible en: https://eur-lex.europa.eu/eli/reg/2023/1114/oj

Parlamento Europeo y Consejo, 2012, 12 de diciembre. Reglamento (UE) 1215/2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (Bruselas I bis). *DOUE* [en línea], L 351/1. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32012R1215

Parlamento Europeo y Consejo, 2016, 27 de abril. Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos, RGPD). *DOUE* [en línea], L 119/1. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios.

BOE [en línea], 287. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2007-20555

Jurisprudencia

Juzgado de lo Mercantil N.º 9 de Barcelona, 11 de enero de 2024. Sentencia del caso *VEGAP v Mango* (SJM B 1/2024), ECLI:ES: JMB:2024:1. Diario del Derecho [en línea], 26 de junio. Disponible en: https://www.iustel.com/diario_del_derecho/noticia.asp?ref_iustel=1256346

Yuga Labs, Inc. v Ryder Ripps 3 [en línea]. Noticia. 6 de septiembre de 2025. Disponible en: https://enriqueortegaburgos.com/yuga-labs-vs-ryder-3/#google_vignette