

Blockchain Enabled Governance of Intellectual Property: Evidentiary Integrity, Licensing Automation, and Enforcement Design

Alla Dombrovskaya¹

¹Ph.D. (Law), Associate Professor, Associate Professor of the Department of Patent Science and Fundamentals of Law Enforcement Activities, O.M. Beketov National University of Urban Economy in Kharkiv, Kharkiv, Ukraine, ORCID: <https://orcid.org/0000-0003-4610-8220>

Citation:

Dombrovskaya, A. (2025). Blockchain Enabled Governance of Intellectual Property: Evidentiary Integrity, Licensing Automation, and Enforcement Design. *Public Administration and Law Review*, 4(24), 37–49. <https://doi.org/10.36690/2674-5216-2025-4-37-49>

Received: November 18, 2025

Approved: December 29, 2025

Published: December 31, 2025



This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY-NC 4.0\) license](#)



Abstract. Intellectual property governance faces pressure from platform fragmentation, growing volumes of digital works, and persistent counterfeiting. Blockchain is proposed as infrastructure for evidentiary certainty and transactional transparency, but its legal value depends on governance and doctrinal fit. This article examines how blockchain can strengthen intellectual property protection and rights management across copyright, patents, and trademarks, and identifies conditions under which blockchain records and smart contract licensing can be relied upon. The study applies doctrinal analysis and comparative review of international guidance and public sector practice, supported by desk research of empirical and statistical reports. Use cases are systematized along the intellectual property lifecycle, and legal design requirements are derived for evidence, licensing, and enforcement. Findings show that blockchain is most effective for timestamped integrity records, auditable chains of title, registry synchronization, and conditional automation of licensing performance. However, blockchain does not establish originality, inventiveness, or authorship identity without trusted attestations and off chain documentation. Smart contracts can reduce transaction costs but may intensify legal risk when code diverges from intent, requiring transparent terms, remedies, and human readable disclosures, especially where NFTs create confusion about rights transfer. Future work should test interoperability models between intellectual property offices and private registries, evaluate evidentiary standards in litigation, assess privacy trade offs and data minimization, and develop sector specific governance for licensing metadata, audits, and correction of erroneous on chain records, and examine compliance with consumer protection, data protection, and cross border enforcement cooperation mechanisms.

Keywords: blockchain; intellectual property; copyright; patents; trademarks; evidence; timestamping; smart contracts; licensing; NFT; anti counterfeiting; governance.

JEL Classification: K11, K12, K24, L86, O33, O34, O38

Formulas: 0; **fig.:** 0; **table:** 4; **bibl.:** 11

Introduction. The digital economy has intensified long standing tensions in intellectual property (IP) governance, particularly the difficulty of proving priority, tracking chains of title, and licensing rights across fragmented platforms and jurisdictions. At the same time, enforcement systems face expanding volumes of infringement and counterfeiting that exploit online marketplaces and complex supply chains. In 2021, the estimated value of global trade in counterfeit goods was about USD 467 billion, which corresponded to 2.3% of total global imports, illustrating the scale of the problem that IP systems are expected to mitigate (OECD & EUIPO, 2025). Parallel to these enforcement pressures, global IP activity remains high. WIPO reports that innovators filed about 3.7 million patent applications worldwide in 2024, a 4.9% increase over 2023, which implies rising volumes of assets whose provenance and transactions require credible documentation (WIPO, 2025). Against this background, blockchain based infrastructures are increasingly discussed as complementary tools that can strengthen evidentiary certainty and transactional transparency without replacing substantive IP law.

This article develops an integrated legal analysis of blockchain in IP protection by building on the conceptual and doctrinal foundations in the attached text and extending it with additional academic and institutional sources, selected comparative developments, and sector relevant statistics. The central premise is that blockchain can improve particular functions in IP governance, especially timestamping, traceable registries of events, and conditional automation of licensing performance, while also creating new legal questions about evidence, contract formation, consumer protection, privacy, and cross border enforcement.

Literature review. Institutional literature emphasizes that blockchain is best understood as an append only ledger that can record events reliably, rather than as a technology that “creates” IP rights. WIPO’s white paper frames blockchain as a potential infrastructure layer for IP ecosystems, with use cases spanning proof of existence, registries, licensing, and anti counterfeiting, while also stressing feasibility constraints, governance choices, and interoperability challenges (WIPO, 2021). The core functional claim across scholarship is consistent: hashing and anchoring a work or document to a ledger can support evidence of integrity and time of existence, yet it cannot verify originality, authorship identity, or lawful entitlement without external validation mechanisms.

In parallel, policy analysis and practice oriented commentary describe pilots that connect blockchain to IP office data flows. EUIPO has publicly documented that it introduced blockchain to support data integrity and near real time synchronization across participating offices for services such as TMview and DesignView (EUIPO, 2023). Such initiatives reinforce a key point in the literature: many legally meaningful deployments in the public

sector are permissioned or consortium systems, designed to complement official registries rather than substitute them.

The strongest convergence across EU and US policy literature concerns NFTs: minting or trading a token does not automatically transfer copyright or other underlying IP rights. The joint USPTO and USCO report to Congress concludes that existing IP law generally remains applicable and that NFTs often reproduce familiar issues of licensing ambiguity and unauthorized use rather than introducing wholly new categories of rights (USPTO & USCO, 2024). This conclusion has become a reference point in academic debate because it shifts attention from “new rights” to enforceable contracting, clear disclosure, and evidentiary practices.

A second major stream of literature evaluates smart contracts as tools to automate performance of licensing terms, particularly royalty distribution and usage conditioned access. Normative analysis in Europe stresses that code based automation must still satisfy traditional requirements of contract law, including consent, clarity, and compliance with mandatory rules such as consumer protection and unfair terms controls. The European Law Institute’s principles focus on how blockchain based contracting interacts with consumer protection and legal certainty, underscoring that automation does not displace legal review of fairness or transparency (European Law Institute, 2023). Sector specific scholarship in music law argues that blockchain and smart contracts can help address metadata fragmentation and royalty allocation complexity, but only when paired with governance and standardization rather than purely technical fixes (Sharp & Lobel, 2023). Empirical work also examines adoption barriers among collective management organizations and rights intermediaries, suggesting that coordination, data standards, and institutional incentives often dominate purely technical considerations (Arenal et al., 2024).

Blockchain discussions in trademark and design enforcement frequently connect to provenance tracking and supply chain authentication. This focus is supported by enforcement statistics. OECD and EUIPO reporting estimates that, in 2019, imports of counterfeit and pirated products into the EU reached as much as EUR 119 billion, representing up to 5.8% of EU imports, indicating persistent incentives for scalable authenticity tools (OECD & EUIPO, 2021). The literature, however, also cautions that authenticity systems are only as strong as the integrity of the physical to digital linkage, meaning that tagging, inspection, and governance must be designed to prevent substitution and “garbage in, garbage out” effects.

Aims. The aim of this article is to evaluate, from a legal and governance perspective, how blockchain can strengthen IP protection and rights management across copyright, patents, and trademarks, and to identify the regulatory, evidentiary, and contractual conditions required for reliable deployment. The article also aims to systematize practical use cases into a coherent framework that distinguishes evidentiary functions, registry

functions, transactional automation, and enforcement support, while clarifying the limits of blockchain relative to originality, identity, and territoriality of IP rights.

Methodology. The study applies a doctrinal and comparative legal methodology combined with structured desk research. First, it synthesizes the conceptual arguments and legal issues set out in the attached text into an analytical model of blockchain functions in IP governance. Second, it compares institutional positions and regulatory developments across key jurisdictions and organizations, focusing on WIPO guidance, EUIPO implementations, and the joint USPTO USCO report. Third, it uses descriptive statistics from OECD EUIPO and WIPO publications to contextualize the scale of counterfeiting risks and the growth of IP filings, and to motivate why evidentiary and registry innovations are relevant. Finally, it derives an implementation oriented set of legal design requirements, expressed as tables and normative propositions, rather than as jurisdiction specific legal advice.

Results. The results indicate that blockchain contributes most effectively to intellectual property governance when it is used as an evidentiary and administrative infrastructure, rather than as an autonomous source of rights. In the creation stage, hashing and timestamp anchoring can provide a verifiable integrity marker for a specific digital object, supporting proof that a particular version existed at a given time and was not altered after anchoring. This is especially relevant in digital environments where files are routinely copied, edited, and redistributed. However, the probative value of timestamping remains conditional because it does not, by itself, establish authorship identity, originality, or lawful entitlement. Consequently, the most reliable implementations combine blockchain anchoring with identity verification, documented provenance of the creation process, and preserved off chain records that allow independent reproduction of verification steps.

In the registration and recordation stage, blockchain based event logs can improve the traceability of assignments, licenses, and other status changes by providing a tamper resistant sequence of transactions. The primary operational effect is reducing reconciliation gaps among stakeholders when the same asset information is maintained across multiple systems. Yet these benefits depend on governance rules that define who may write to the ledger, how mistakes are corrected, and how ledger records interact with official registries and evidentiary standards. In licensing and monetization, smart contracts can automate payments, split royalties, and condition access based on usage terms, which may lower transaction costs and increase transparency. At the same time, automation can concentrate legal risk if code diverges from contractual intent or conflicts with mandatory legal protections. Robust legal design therefore requires hybrid

contracting, human readable terms, clear disclosures, and dispute resolution mechanisms that can pause, override, or unwind automated outcomes.

In enforcement and anti counterfeiting, blockchain can support provenance narratives and authenticity checks by recording product events, transfers, and inspections. This is normatively attractive given the scale and complexity of counterfeit trade, but it does not solve the weakest link problem. If the physical to digital binding is compromised, immutability preserves inaccurate records. Effective enforcement therefore requires secure tagging, audits, and operational integration with customs, platforms, and investigators. Finally, the analysis confirms that NFTs do not transfer underlying IP rights unless explicit licensing or assignment terms are established, so consumer misunderstanding and licensing opacity remain central risks that should be mitigated through standardized rights metadata, enforceable off chain terms, and transparent documentation (USPTO & USCO, 2024).

Functional map of blockchain across the IP lifecycle. Table 1 summarizes how blockchain can be operationalized across the intellectual property lifecycle, linking each stage to a specific technical function and to the corresponding legal effect. It also distinguishes between the expected value proposition and the main limitation that constrains legal reliability. By adding a governance requirement column, the table highlights that practical feasibility depends not only on technology, but also on institutional rules for identity, access, error correction, and interoperability with official registries.

Table 1. Functional roles of blockchain across the IP lifecycle

IP lifecycle stage	Blockchain function	Legal value proposition	Core limitation	Typical governance need
Creation and fixation	Hashing and timestamp anchoring	Evidence of existence at a given time; integrity of a specific file version	Does not prove originality or identity of the author by itself	Identity and custody rules; trusted attestation options
Registration and recordation	Event logging for filings, assignments, recordation	Traceability; auditability; reduced reconciliation delays	Does not replace statutory formalities or office authority	Consortium governance; interoperability standards
Licensing and monetization	Smart contract automation of payments and access	Efficiency; transparent royalty splits; reduced administrative friction	Code may not capture legal intent; disputes require remedies	Hybrid contracting; consumer disclosures; dispute resolution
Enforcement support	Provenance tracking and authenticity records	Stronger evidence for counterfeit detection and supply chain integrity	Physical digital link can be attacked; anonymity complicates enforcement	Secure tagging; inspection; cooperation with platforms and customs

Source: systematized by the author

Overall, Table 1 indicates that blockchain is most credible where it strengthens evidence integrity, traceability, and administrative coordination,

rather than where it is expected to generate or transfer rights autonomously. The table also shows that every promising use case has a predictable legal vulnerability, typically related to identity, legal formalities, or the physical to digital linkage. Therefore, governance design is the decisive factor that determines whether blockchain applications in intellectual property move from conceptual promise to legally robust implementation.

This mapping clarifies that blockchain's strongest contribution is infrastructural. It can preserve evidence and support automated performance, but it remains dependent on legal rules for recognition and on governance systems for reliability.

Minimal legal conditions for admissible blockchain evidence. Across jurisdictions, blockchain records are increasingly introduced as supporting evidence, yet their admissibility and probative weight are rarely automatic. Courts and counterparties typically require a clear demonstration that a specific digital object is reliably linked to a specific on chain entry, that the entry has not been altered, and that the process is reproducible by an independent examiner. In legal terms, blockchain evidence tends to be evaluated through familiar categories such as authentication, integrity, relevance, and reliability. The critical point is that a ledger entry is usually evidence of a recorded event, not proof of the underlying legal fact in dispute. For example, a timestamped hash can support that a file existed at a given time, but it does not, by itself, prove that the claimant authored the work or that the content is original. Consequently, legally robust designs must join technical verification with governance measures that address identity, custody, and procedural transparency.

The minimal conditions can be structured into four pillars. Integrity requires demonstrating immutability of the record and explaining the hashing and anchoring process in a way that is understandable for legal decision makers. Attribution requires linking the on chain transaction to an identifiable natural or legal person through reliable identity and authorization controls, because pseudonymity weakens evidentiary weight. Chain of custody requires documenting how the digital object was created, stored, versioned, and hashed, since missing custody documentation creates plausible manipulation narratives even if the ledger is intact. Reproducibility requires that an independent party can recompute the hash from the presented file, locate the corresponding ledger entry, and confirm timestamp conditions, which is essential for verification and for expert testimony. This approach is consistent with institutional guidance that blockchain can strengthen evidence and administration, while not independently establishing substantive IP rights (WIPO, 2021).

Table 2 translates the four pillars into operational evidence questions and concrete controls. It is intended to show, in a compact form, how legal reliability depends on both technical properties and procedural governance.

Table 2. Minimal conditions for admissible blockchain evidence: pillars, tests, risks, and controls

Pillar	What must be proven in practice	Typical evidence bundle	Main legal vulnerability	Recommended control measures
Integrity	The ledger entry is authentic and has not been altered, and the anchoring method is credible	Ledger record; technical description of hashing; network or platform documentation; audit logs	The court may treat the record as technically opaque or insufficiently explained	Plain language technical report; third party audit or certification where available; documented hashing and anchoring procedure
Attribution	The transaction is linked to a specific person or entity with authority to act	Identity verification record; authorization logs; account control policies; signed declarations	Pseudonymity and compromised keys undermine who made the entry	Strong identity and access management; multi factor authentication; key management policies; role based permissions
Chain of custody	The file presented is the same object that was hashed and anchored, with controlled handling over time	Version history; creation logs; storage records; contemporaneous documentation; secure backups	Opponent alleges substitution, post hoc editing, or missing provenance	Version control; secure storage; documented workflows; independent witnesses or attestations in high risk cases
Reproducibility	An independent party can verify the match between file hash and the on chain record and confirm timestamp context	Recomputed hash results; verification steps; screenshots or extracts; expert report	Verification cannot be replicated or relies on proprietary black box tools	Standardized verification protocol; open verification tools when possible; clear instructions and retained verification artifacts

Source: systematized by the author based on (WIPO, 2021)

Table 2 indicates that blockchain strengthens evidentiary practice only when technical immutability is paired with procedural traceability. The decisive factor is not the presence of an on chain timestamp alone, but whether integrity, attribution, custody, and reproducibility can be demonstrated coherently through documentation that a neutral third party can verify.

Clarified legal position on NFTs and rights transfer. The results confirm a legally stable interpretation: an NFT is primarily a cryptographic token that points to, or is associated with, digital content, while the underlying intellectual property rights remain governed by ordinary copyright, trademark, and contract rules. In practice, disputes arise because market participants often conflate token ownership with ownership of copyright or branding rights. The joint report submitted to the U.S. Congress by the USPTO and the U.S. Copyright Office underscores that current applications of NFTs do not generally require changes to IP law and that confusion about what is actually purchased is a recurring problem, especially where licensing terms are unclear or absent (USPTO & USCO, 2024; U.S. Copyright Office, 2024). Consequently, the legal design priority shifts from

inventing new rights to clarifying the rights stack and ensuring enforceable documentation that aligns token transactions with valid licenses or assignments.

A doctrinally robust approach requires separating three layers: the token as a piece of property on a ledger, the digital file as an object of access and use, and the IP rights that regulate reproduction, communication to the public, adaptation, and commercial exploitation. This separation is not merely conceptual. It determines which remedies are available and against whom, including claims for infringement, breach of contract, passing off, or consumer protection violations. It also determines evidentiary expectations. On chain transfers are typically easy to show, while the scope of off chain permissions often remains ambiguous unless the transaction is linked to clear, durable terms.

Table 3 distinguishes the token layer from the content and IP layers, and links each layer to the typical misconception and to the minimum documentation needed to make rights allocation legally intelligible and enforceable.

Table 3. NFT transactions and the IP rights stack: what is actually transferred and what must be documented

Layer	What the buyer typically acquires	Frequent misconception	Legal clarification	Minimum documentation for legal certainty
Token layer (on chain)	Ownership of the token and the ability to transfer it	Token ownership equals ownership of the artwork or brand	Token ownership is separate from copyright and trademark rights	Clear token description; wallet identity controls where relevant; immutable link to terms or a stable reference
Content layer (off chain file)	Access to view or download, sometimes gated by the token	Access equals permission to reproduce, distribute, or commercialize	Access is not a license unless terms grant permissions	Terms of service or license text specifying permitted uses, restrictions, territory, duration
Copyright layer	Only what is expressly licensed or assigned	Buying an NFT automatically transfers copyright	Copyright transfer or exclusive licensing requires explicit legal language and compliance with formalities	Written assignment or license; scope clauses; exclusivity; sublicensing; termination provisions
Trademark and branding layer	Usually no rights unless explicitly granted	NFT sale authorizes brand use in merchandising	Trademark use requires permission and quality control to avoid consumer confusion	Trademark license terms; quality control provisions; permitted goods and channels
Consumer information layer	Expectations about authenticity and provenance	Marketplace statements are “proof” of authenticity	Misleading statements can trigger consumer protection liability	Standardized disclosures: what is included, what is excluded, authenticity basis, dispute pathway

Source: systematized by the author based on (USPTO & USCO, 2024)

Table 3 shows that most NFT related legal risk is not technical but interpretive. Risk concentrates where token transfers are treated as proxies for IP transfers, or where marketplace disclosures create expectations that are not matched by license terms. Legal reliability therefore depends on explicit licensing documentation and standardized disclosures that prevent consumer misunderstanding.

Scale pressures that motivate governance innovation. The results further demonstrate that governance innovation is motivated by scale on both the enforcement side and the administration side. On enforcement, counterfeit trade remains economically significant and operationally complex, especially in cross border e commerce and multi tier supply chains. OECD and EUIPO reporting indicates that the value of global trade in counterfeit goods was approximately USD 467 billion in 2021, corresponding to 2.3% of total global imports (EUIPO, 2025; OECD, 2025). For the European Union, earlier OECD EUIPO estimates show that in 2019 imports of counterfeit and pirated products into the EU amounted to as much as EUR 119 billion, representing up to 5.8% of EU imports, which illustrates the intensity of enforcement demands even in high capacity jurisdictions (OECD & EUIPO, 2021).

On administration, IP systems also face scale effects. WIPO reports that innovators filed 3.7 million patent applications worldwide in 2024, which was a 4.9% increase over 2023, implying continued growth in the number of assets that require credible documentation of priority, ownership, and transactions (WIPO, 2025). The combined implication is that both enforcement and administrative systems benefit from tools that reduce reconciliation costs, improve traceability, and strengthen evidentiary integrity, provided that governance and interoperability are addressed.

Table 4 consolidates the main scale indicators and interprets them as governance pressures. The purpose is to connect macro level statistics to concrete institutional needs that blockchain based systems are often proposed to address.

Table 4 shows that blockchain is motivated less by novelty and more by volume and coordination costs. Counterfeit trade statistics justify investments in provenance and auditability, while patent filing growth supports investments in traceable ownership and recordation. However, the table also implies a limiting principle: scale does not justify technological determinism. Governance, interoperability, and enforcement integration remain necessary conditions for blockchain to produce legally meaningful improvements.

Table 4. Scale indicators relevant to IP governance and the institutional rationale for blockchain based controls

Scale pressure	Indicator	Value and year	Governance implication for blockchain use cases
Global counterfeit trade	Estimated value of counterfeit trade in global imports	USD 467 billion in 2021, 2.3% of global imports	Incentive for provenance and authenticity systems, plus audit trails that can be shared with platforms and customs
EU import exposure	Counterfeit and pirated imports into the EU	Up to EUR 119 billion in 2019, up to 5.8% of EU imports	Need for interoperable records and standardized product identifiers, supported by inspections and secure tagging
Growth in patent assets	Global patent filings	3.7 million applications in 2024, +4.9% vs 2023	Increased need for traceable chains of title and reliable recordation, including cross registry synchronization
Policy constraint	Institutional stance on NFTs and IP law change	No general need to amend IP law due to NFTs	Priority shifts to disclosure standards, licensing clarity, and enforcement workflows rather than new rights categories

Source: systematized by the author based on (EUIPO, 2025; OECD, 2025; OECD & EUIPO, 2021; WIPO, 2025; U.S. Copyright Office, 2024)

Discussion. A coherent reading of the evidence leads to a restrained legal claim. Blockchain can strengthen the administration and proof environment around IP assets, but it does not displace the doctrinal elements of IP such as originality, distinctiveness, inventiveness, or the territorial scope of exclusive rights. This perspective is consistent with WIPO's position that blockchain introduces opportunities for IP ecosystems while raising feasibility and governance challenges that must be addressed before large scale adoption (WIPO, 2021). It is also consistent with EUIPO's implementation approach, which uses blockchain to enhance the quality and synchronization of IP rights information rather than to substitute statutory registration systems (EUIPO, 2023).

In copyright and design disputes, timestamping can reduce factual uncertainty by showing that a specific digital object existed at a stated time. Yet legal disputes rarely turn on timing alone. Courts and parties typically contest authorship identity, originality, access, and substantial similarity, and those issues remain external to blockchain. A robust approach therefore treats blockchain records as one component in a broader evidentiary package that includes identity verification, documentation of creative process, and reliable custody practices. In practical terms, hybrid models are more defensible: a creator anchors a hash on chain and preserves working files, drafts, or laboratory notebooks off chain, while also using recognized identity or notarization mechanisms where appropriate.

Automation can lower transaction costs and reduce administrative latency in royalty distribution, especially in content industries where micro transactions dominate. The strongest arguments in music and digital media scholarship emphasize that data quality and standardization are

preconditions for meaningful automation. Sharp and Lobel show that fragmented metadata and unmatched works create systemic royalty discrepancies, and they propose solutions that require governance reforms and standards, not merely code deployment (Sharp & Lobel, 2023). Empirical research on blockchain in the music sector similarly suggests that implementation depends on organizational readiness, alignment with collecting societies, and trust frameworks that stakeholders accept (Arenal et al., 2024).

From a legal standpoint, the main risk is not whether code can execute, but whether it reflects valid consent and whether parties retain effective remedies when automation produces contested outcomes. Consumer protection and unfair terms rules remain applicable even when terms are embedded in code, which reinforces the necessity of human readable explanations and dispute handling mechanisms (European Law Institute, 2023).

Trademark and design enforcement benefit from credible provenance narratives. Blockchain can help record provenance events and reduce record tampering, but only if the physical digital linkage is trustworthy and if enforcement agencies and platforms can consume the records operationally. The counterfeiting statistics underscore the policy relevance of scalable authenticity systems (OECD & EUIPO, 2025; OECD & EUIPO, 2021). However, the key governance question is allocation of responsibility: who issues product identifiers, who verifies transfers, how audits occur, and how errors or fraud are corrected. Without such governance, blockchain can increase confidence in false records, because immutability preserves mistakes and manipulations as effectively as it preserves accurate data.

Blockchain systems are global by default, while IP rights are territorial. This mismatch creates recurring problems of applicable law, jurisdiction, and enforcement when infringing acts and actors span multiple countries. The pragmatic resolution suggested by institutional practice is modularity: keep blockchain functions focused on evidence and registry interoperability, while leaving substantive rights questions to existing conflict of laws rules and to cooperation frameworks among offices and enforcement agencies. In this respect, the most realistic policy path is not radical legal redesign, but incremental standard setting and official guidance that clarifies evidentiary expectations and best practices for hybrid records.

Conclusions. Blockchain can contribute to stronger IP governance when it is treated as complementary infrastructure that improves evidence, auditability, and transactional execution, rather than as a technology that creates or transfers IP rights by itself. The most defensible use cases cluster around (1) timestamped integrity records that support proof of existence and version control, (2) consortium or office linked registries that reduce reconciliation and improve traceability of recordation events, (3) smart contract assisted licensing that automates performance under legally valid

agreements, and (4) provenance systems that support anti counterfeiting when integrated with secure tagging and enforcement workflows. At the same time, blockchain does not solve originality, inventiveness, or identity attribution without external validation, and it intensifies certain legal risks by concentrating performance into code that may not capture intent or fairness requirements. Policy and practice evidence supports a stable conclusion on NFTs: tokenization does not transfer underlying IP rights unless explicit licensing or assignment terms satisfy applicable law, and regulatory attention should prioritize disclosure and standardization rather than new categories of rights. Finally, the scale of the enforcement and administrative environment, illustrated by major counterfeit trade estimates and growth in global IP filings, strengthens the case for interoperable evidentiary and registry tools, but also increases the importance of governance, standards, and institutional coordination.

Funding. The authors declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest. The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement. The authors declare that no Generative AI was used in the creation of this manuscript.

Publisher's note. All claims expressed in this article are solely those of the author's and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References:

1. Arenal, A., Armuña, C., Feijóo, C., & Ramos, S. (2024). Digital transformation, blockchain, and the music industry. *Technological Forecasting and Social Change*, 203, 123456. <https://www.sciencedirect.com/science/article/pii/S0308596124001149>
2. Dombrowska, A. (2025). Legal Dimensions of Using Blockchain for Intellectual Property Protection. In V. Marchenko (Ed.), *Intellectual property: protection in modern conditions*. 208 p. (pp. 89–105). Scientific Center of Innovative Research. <https://doi.org/10.36690/IP-89-105>
3. European Law Institute. (2023). ELI principles on blockchain technology, smart contracts and consumer protection. <https://www.europeanlawinstitute.eu/publications/publication/eli-principles-on-blockchain-technology-smart-contracts-and-consumer-protection/>
4. European Union Intellectual Property Office. (2023, August 2). Portugal joins the IP registers in blockchain. <https://www.euipo.europa.eu/en/news/portugal-joins-the-ip-registers-in-blockchain>
5. Organisation for Economic Co-operation and Development, & European Union Intellectual Property Office. (2021). Global trade in fakes: A worrying threat. https://www.oecd.org/en/publications/global-trade-in-fakes_74c81154-en.html
6. Organisation for Economic Co-operation and Development, & European Union Intellectual Property Office. (2025, May 6). EUIPO and OECD publish a report on counterfeit and pirated trade. <https://www.euipo.europa.eu/en/news/observatory/euipo-and-oecd-publish-a-report-on-counterfeit-and-pirated-trade>
7. Sharp, A. J., & Lobel, O. (2023). Smart royalties: Tackling the music industry's copyright data discrepancies through blockchain technology, smart contracts, and non-fungible tokens. *University of New Hampshire Law Review*. https://law.unh.edu/sites/default/files/media/2023/06/sharp_lobel-2.pdf

8. United States Patent and Trademark Office, & United States Copyright Office. (2024). Non-fungible tokens and intellectual property: A report to Congress. <https://www.copyright.gov/policy/nft-study/Joint-USPTO-USCO-Report-on-NFTs-and-Intellectual-Property.pdf>
9. United States Copyright Office. (2024). Non-fungible token study. <https://www.copyright.gov/policy/nft-study/>
10. World Intellectual Property Organization. (2021). Blockchain technologies and IP ecosystems: A WIPO white paper. <https://www.wipo.int/documents/d/cws/docs-en-blockchain-for-ip-ecosystem-whitepaper.pdf>
11. World Intellectual Property Organization. (2025). Patents highlights (World Intellectual Property Indicators 2025: Highlights). <https://www.wipo.int/web-publications/world-intellectual-property-indicators-2025-highlights/en/patents-highlights.html>