

Hybrid Governance of Intellectual Property in the Digital Age: Aligning Law, Platforms, AI, and Blockchain for Effective Protection

Inna Kilimnik¹

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/0000-0003-3225-6257>

Citation:

Kilimnik, I. (2025). Hybrid Governance of Intellectual Property in the Digital Age: Aligning Law, Platforms, AI, and Blockchain for Effective Protection. *Public Administration and Law Review*, 4(24), 60–67. <https://doi.org/10.36690/2674-5216-2025-4-60-67>

Received: November 19, 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. Accelerated digitalisation is reshaping how intellectual property is created, exploited, and protected, while exposing the limits of classical doctrines, especially territoriality and conventional enforcement models. Platform markets, data-intensive business models, AI-enabled replication, and distributed technologies amplify cross-border circulation of protected subject matter and increase the evidentiary and cybersecurity burdens placed on rights holders and institutions. The study aims to develop a governance-oriented model of IP protection in the digital environment that integrates legal harmonisation, platform accountability, cybersecurity safeguards, and the conditional use of emerging technologies such as blockchain, smart contracts, and AI-enabled detection. The article applies formal-legal and comparative analysis of European and international instruments, complemented by system-structural mapping of the IP lifecycle to connect platform and AI vulnerabilities with governance controls such as authentication, auditability, interoperability, and remedies. Secondary statistics are used to contextualise scale and enforcement pressure. The results show that the most destabilising effect of digitisation is institutional: disputes increasingly depend on evidence quality, platform procedures, and security posture rather than on doctrinal entitlement alone. Blockchain contributes most reliably when treated as evidentiary and administrative infrastructure, because timestamping and hashing support integrity markers but do not prove authorship or lawful entitlement without identity, provenance, and reproducible verification. NFTs are not rights-transfer mechanisms absent explicit licensing or assignment terms. Effective digital-age IP protection requires a hybrid governance model combining procedural clarity, institution-building, cybersecurity maturity, and carefully scoped technology deployment. Future studies should test admissibility pathways for blockchain-supported evidence, evaluate interoperability designs for registries and platforms, and measure error and remedy performance in automated enforcement pipelines.

Keywords: intellectual property governance; platform accountability; digital evidence; interoperability; cybersecurity; blockchain anchoring; smart contracts; NFT licensing; AI-enabled infringement; provenance; enforcement scalability; hybrid regulation.

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

Formulas: 0; **fig.:** 0; **table:** 3; **bibl.:** 15

Introduction. Accelerated digitalisation has changed how intellectual property is created, exploited, and protected, while also exposing structural limits of classical doctrines, especially territoriality and conventional enforcement models.

Platform-based markets, data-intensive business models, and the diffusion of artificial intelligence and distributed technologies intensify cross-border circulation of protected subject matter, increase the scale of infringement, and add cybersecurity risks that were not central to earlier IP paradigms.

These shifts are observable in the growth of global innovation activity: in 2024, worldwide patent filings reached 3.7 million, a 4.9% increase over 2023. In parallel, enforcement operates under scale pressure: global counterfeit trade has been estimated at about USD 467 billion for 2021, or 2.3% of global imports, illustrating the persistent economic incentives for illicit replication and distribution.

Against this background, contemporary IP protection increasingly requires an integrated approach that combines legal harmonisation, institutional capacity, and technological safeguards rather than relying on legal doctrine alone.

The article develops a governance-oriented synthesis that connects EU regulatory trajectories, evidence standards for digital records, platform accountability, and practical conditions for deploying blockchain, watermarking, and AI-enabled enforcement tools in a legally reliable manner.

Literature review. Scholarship on digital transformation and IP protection has developed along several complementary lines. First, socio-legal and political economy perspectives emphasise how networked infrastructures reshape governance, regulatory power, and market organisation, which indirectly alters the functioning of IP institutions. Second, core IP scholarship has analysed how digitisation undermines assumptions about scarcity, distribution control, and enforceability, and why recalibration is needed to balance innovation incentives with public interest safeguards. Third, cybersecurity and digital governance literature highlights that confidentiality, integrity, and availability of digital assets are now central to IP resilience, especially for trade secrets and high-value R&D.

In the EU context, regulatory developments increasingly affect IP enforcement through horizontal platform governance and digital market rules. The Digital Services Act establishes due-diligence and risk management expectations for certain online intermediary services, shaping notice-and-action and systemic risk approaches that intersect with IP complaints. The AI Act introduces obligations for AI systems and, for certain general-purpose AI models, transparency-related requirements that can interact with IP-relevant concerns such as training data governance and disclosure practices. Copyright modernisation in the EU also remains

anchored in the InfoSoc Directive (2001/29/EC) and the DSM Directive (2019/790), which address digital uses and platform-mediated dissemination. For enforcement, the IPR Enforcement Directive (2004/48/EC) continues to structure civil remedies and evidentiary mechanisms across Member States.

A fourth stream addresses technological instruments. WIPO's work on blockchain and IP ecosystems catalogues potential applications while stressing governance, interoperability, and legal recognition as decisive constraints. Policy analyses of NFTs and IP similarly converge on a stabilised conclusion: tokenisation does not itself transfer underlying IP rights absent explicit licensing or assignment terms, and consumer confusion about "what is purchased" remains a core governance risk. Taken together, the literature supports a shift from technology optimism to institutionally grounded design, where tools are evaluated by evidentiary reliability, accountability, and compatibility with existing legal procedures.

Aims. The aim of this article is to develop a structured, governance-oriented model of IP protection in the digital environment that integrates legal harmonisation, platform accountability, cybersecurity safeguards, and the conditional use of emerging technologies (blockchain, smart contracts, watermarking, AI-enabled detection).

Methodology. The study applies a combined legal and interdisciplinary methodology. It relies on formal-legal analysis of international and European instruments relevant to IP and digital governance, and on comparative reasoning to identify regulatory patterns that can generalise across jurisdictions.

System-structural analysis is used to map the IP lifecycle, identify points of vulnerability created by platforms and AI pipelines, and connect those vulnerabilities to governance controls (authentication, audit, interoperability, remedies).

Empirical support is incorporated through secondary statistics from authoritative sources, including WIPO's indicators on global filing activity and OECD–EUIPO estimates on counterfeit trade. The methodology is intentionally design-oriented: it evaluates technology instruments not as substitutes for legal rights, but as infrastructural components whose value depends on admissibility, attribution, chain of custody, and institutional integration.

Results. Digital transformation pressures IP systems through platformisation, AI generation and replication, data extraction for training, and the securitisation of IP as a cybersecurity target.

These drivers do not merely add new infringement channels; they alter how evidence is produced, how liability is allocated across intermediaries, and how rights are operationalised in automated environments.

Table 1 summarises the main digital drivers and specifies which legal layer is primarily stressed, distinguishing substantive law questions from enforcement and evidence questions.

Table 1. Digital drivers and principal legal stress points

Digital driver	Typical IP exposure	Primary legal stress point	Practical implication
Platformisation (streaming, marketplaces, social media)	Mass distribution, repeat infringement, counterfeit sales	Intermediary responsibility; cross-border enforcement	Enforcement shifts toward platform procedures and scalable notice-and-action governance
Data extraction and scraping	Unauthorised copying for analytics and model training	Scope of permissible uses; licensing; evidence	Disputes increasingly depend on dataset provenance and audit trails
Generative AI content and replication	Style imitation, synthetic works, automated derivative creation	Authorship and originality concepts; attribution	Enforcement becomes mixed: copyright, unfair competition, and consumer protection pathways
Trade secrets in networked firms	Cyber-espionage, insider leaks, supply-chain compromise	Reasonable secrecy measures; cybersecurity controls	IP protection becomes co-dependent on security governance and incident response
Tokenisation (NFTs)	Confusion about rights transfer; licensing opacity	Contract clarity; consumer understanding	NFTs do not transfer IP rights without explicit terms

Source: systematized by the author

The mapping shows that the most destabilising effect of digitisation is institutional: disputes are increasingly decided by evidence quality, platform process design, and cybersecurity posture, not only by doctrinal entitlement.

The analysis supports a consistent conclusion: blockchain is most valuable for IP governance when treated as evidentiary and administrative infrastructure, not as an autonomous source of rights. In creation and fixation, hashing and timestamp anchoring can establish an integrity marker for a specific digital object and support documentary continuity across distributed workflows. However, timestamping alone does not prove authorship identity, originality, or lawful entitlement, so robust implementations require identity verification, provenance documentation, and preserved off-chain records to reproduce verification in disputes.

In registration and recordation, tamper-resistant event logs can improve traceability of assignments and licences and reduce reconciliation gaps between stakeholders, but only where governance rules specify write-access, correction procedures, and interoperability with official registries and evidence practices. In licensing and monetisation, smart contracts can automate payments and royalty splits and reduce administrative friction, yet automation concentrates legal risk because code may diverge from contractual intent and mandatory protections, shifting disputes to questions

of interpretation and remedies. In enforcement and anti-counterfeiting, blockchain can support provenance narratives, but it cannot solve the “weakest link” problem: if the physical-to-digital binding is compromised, immutability preserves inaccurate records rather than correcting them.

Table 2 summarises blockchain functions across the IP lifecycle and specifies governance conditions needed for legal reliability.

Table 2. Blockchain roles across the IP lifecycle and the governance conditions for reliability

IP lifecycle stage	Blockchain function	Practical value	Core limitation	Governance condition that determines usefulness
Creation and fixation	Hashing and timestamp anchoring	Integrity marker; evidence of existence at a time	No proof of identity or originality by itself	Identity and custody rules; reproducible verification process
Registration and recordation	Event logging for filings, assignments	Traceability; reduced reconciliation delays	Does not replace statutory formalities	Permissioned governance; interoperability with official registries
Licensing and monetisation	Smart contract execution	Automated royalties; transparency	Code may not reflect intent; remedy gaps	Hybrid contracting; pause and override pathways; dispute resolution design
Enforcement support	Provenance tracking, inspections log	Stronger narratives for authenticity checks	Physical-digital link can be attacked	Secure tagging; audits; integration with customs and platforms

Source: systematized by the author

The table indicates that blockchain becomes legally meaningful only when embedded in accountability structures that support attribution, correction, and enforceable remedies, which aligns with WIPO’s emphasis on governance and feasibility conditions.

Evidence from policy studies confirms that NFTs do not automatically transfer copyright, trademark, or patent rights unless accompanied by explicit licensing or assignment terms that satisfy applicable legal requirements. The regulatory priority is therefore not “recognising NFTs” as a new right, but standardising rights metadata, requiring clear consumer-facing disclosures, and aligning token-market practices with contract and consumer protection rules to reduce misunderstanding about what is bought.

Two statistics illustrate why evidence infrastructure and scalable enforcement processes matter. First, global patent filing volume reached 3.7 million in 2024, signalling persistent growth in formal innovation claims and corresponding administrative load for examination and dispute systems. Second, counterfeit trade estimates at USD 467 billion (2021) underscore the enforcement challenge created by fragmented supply chains and online marketplaces, where authenticity and provenance are difficult to verify at scale.

Table 3 links these scale indicators to governance implications, showing what each number implies for institutions rather than treating statistics as descriptive only.

Table 3. Selected scale indicators and governance implications

Indicator	Latest value (source)	Governance implication for IP protection
Global patent applications	3.7 million (2024)	Administrative capacity, digital filing integrity, and dispute readiness become systemic constraints
Global counterfeit trade estimate	USD 467 billion (2021)	Authentication infrastructure and coordinated enforcement with platforms and customs become priority controls
Trademark application class count	15.2 million (2024)	Brand protection increasingly depends on platform governance and scalable monitoring

Source: systematized by the author

Scale indicators justify why digital evidence, interoperability, and platform-centred enforcement are not optional innovations but structural necessities for IP systems under high-volume conditions.

The synthesis supports the conclusion that IP protection can no longer rely solely on classical legal doctrines, because digital transformation exposes territorial limitations, increases automated infringement, and raises cybersecurity vulnerabilities.

A hybrid governance model integrates: (i) legal harmonisation and procedural clarity, (ii) technological safeguards with reproducible verification, and (iii) international cooperation and institutional capability.

This logic is consistent with the EU's combination of enforcement instruments and horizontal platform governance, including the DSA and related regulatory architecture.

Discussion. The results have three main implications for policy and practice. First, the most important shift is epistemic: the decisive question in many digital IP disputes becomes how reliably a claimant can demonstrate provenance, integrity, and attribution of digital objects and transactions. This reframes technological tools as components of legal fact-finding rather than substitutes for rights.

Second, platform governance becomes central because many infringement flows are mediated by a small number of infrastructures, meaning that enforcement capacity increasingly depends on procedural design, transparency, and accountability expectations for intermediaries.

Third, AI changes both the threat model and the enforcement toolkit: it enables automated copying and convincing synthetic media, while also enabling detection at scale, but both directions raise due process risks if automation produces false positives or opaque decisions.

From a regulatory standpoint, a practical balance can be achieved by aligning technology use with evidence standards and remedy design. Blockchain anchoring and provenance tracking can support integrity claims,

but must be connected to identity verification and correction procedures to avoid preserving erroneous records. Smart contracts can reduce administrative friction, but only when coupled with human-readable terms and robust dispute-resolution pathways that can pause or unwind automated outcomes. NFTs illustrate the same pattern: the governance failure is usually not technological, but contractual opacity and consumer misunderstanding, which is why policy analyses emphasise disclosures and rights clarity rather than creating new IP rules.

The hybrid governance model also clarifies what “institutional capacity” means in digital IP. It includes technical competence in handling electronic evidence, procedural readiness for cross-border cooperation, and cybersecurity maturity to protect registries, trade secrets, and evidence repositories. It also includes interoperability, because fragmented registries and inconsistent metadata prevent scalable verification and encourage reliance on informal platform processes. In this sense, EU-aligned approaches increasingly operate as multi-layer governance systems where civil enforcement, platform due diligence, and technology-based verification must be designed to work together rather than as separate silos.

Conclusions. Digital transformation is not a marginal stressor for IP law; it restructures the conditions of creation, distribution, infringement, and proof, thereby exposing the limits of territorial doctrines and traditional enforcement routines.

The article shows that blockchain and related tools contribute most effectively when they operate as evidentiary and administrative infrastructure embedded in governance rules that secure attribution, reproducibility, interoperability, and remedies. NFTs reinforce the same conclusion: tokenisation is not a rights transfer mechanism without explicit legal terms, so governance must prioritise licensing clarity and consumer disclosures. Scale indicators, including record patent filings and large counterfeit trade volumes, support the argument that IP systems need scalable verification and enforcement processes to remain effective under high-volume digital conditions.

Overall, the most defensible direction is a hybrid model of IP governance that combines legal harmonisation, institutional strengthening, cybersecurity safeguards, and carefully scoped technological instruments.

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. Abbott, R. (2020). *The reasonable robot: Artificial intelligence and the law*. Cambridge University Press. <https://www.cambridge.org/core/books/reasonable-robot/>
2. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets). <https://eur-lex.europa.eu/eli/dir/2016/943/oj>
3. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market. <https://eur-lex.europa.eu/eli/dir/2019/790/oj>
4. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001L0029>
5. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0048>
6. Kilimnik, I. (2025). Contemporary Challenges in Intellectual Property Protection: Legal Transformations and Technological Disruptions. In V. Marchenko (Ed.), *Intellectual property: protection in modern conditions*. 208 p. (pp. 45-67). Scientific Center of Innovative Research. <https://doi.org/10.36690/IP-45-67>
7. Organisation for Economic Co-operation and Development, & European Union Intellectual Property Office. (2025). *Report on counterfeit and pirated trade* (estimate for 2021: USD 467 billion; 2.3% of global imports). <https://www.euipo.europa.eu/en/news/observatory/euipo-and-oecd-publish-a-report-on-counterfeit-and-pirated-trade>
8. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
9. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
10. Stanford Encyclopedia of Philosophy. (2022). *Intellectual property*. <https://plato.stanford.edu/entries/intellectual-property/>
11. United States Copyright Office. (2024). *Non-fungible token study*. <https://www.copyright.gov/policy/nft-study/>
12. United States Patent and Trademark Office, & United States Copyright Office. (2024). *Non-fungible tokens and intellectual property: A report to Congress*. <https://www.uspto.gov/sites/default/files/documents/Joint-USPTO-USCO-Report-on-NFTs-and-Intellectual-Property.pdf>
13. World Intellectual Property Organization. (2021). *Blockchain technologies and IP ecosystems (white paper)*. <https://www.wipo.int/documents/d/cws/docs-en-blockchain-for-ip-ecosystem-whitepaper.pdf>
14. World Intellectual Property Organization. (2025). *Patents highlights: World Intellectual Property Indicators 2025*. <https://www.wipo.int/web-publications/world-intellectual-property-indicators-2025-highlights/en/patents-highlights.html>
15. World Intellectual Property Organization. (2025). *WIPO IP facts and figures 2025*. <https://www.wipo.int/edocs/pubdocs/en/wipo-pub-943-2025-en-wipo-ip-facts-and-figures-2025.pdf>