

Hybrid Authorship and Legal Uncertainty: Rethinking Intellectual Property for AI- Generated and NFT Art

Jeralyn Valencia ^a , Fajar Sugianto ^b  , Atsuko Yamamoto ^c ,
Jerry Shalmont ^a , Nadya Suryo ^d 

^a Faculty of Law, Universitas Pelita Harapan, Tangerang, Indonesia

^b Faculty of Law, Universitas Pelita Harapan, Jakarta, Indonesia

^c Ray of Light Incorporation, Tokyo, Japan

^d Department of Biotechnology and Bioindustry Sciences,
National Cheng Kung University, Tainan, Taiwan

✉ Corresponding email: fajar.sugianto@uph.edu

Abstract

The convergence of artificial intelligence, blockchain, and non-fungible tokens (NFTs) has triggered a doctrinal crisis in copyright, contract, and evidence law across several major jurisdictions, including the United States, the European Union, and selected Asian legal systems. By 2025, over 70% of top NFT sales feature hybrid human–AI creations, yet most remain in legal and economic “gray zones” across jurisdictions. This article examines the challenge of partial AI authorship through a comparative analysis of U.S., EU, and Asian legal frameworks, revealing enduring gaps in originality doctrine, inconsistencies in the treatment of blockchain-based evidence, and contested approaches to smart contract enforceability and royalty mechanisms. Particular attention is given to the technical processes through which AI systems source, transform, and recombine data from public and private domains, raising unresolved questions of infringement, attribution, and authorship when copyrighted works are used without authorization. Drawing on originality doctrine, transformative use standards, and fair use principles, the analysis argues that legal protection should

be confined to AI-assisted outputs that reflect meaningful human creative judgment and demonstrable transformation, rather than automated reproduction. Situating these doctrinal tensions within broader patterns of market volatility, regulatory arbitrage, and unequal access to justice. It concludes that adaptive, pluralist governance is essential to achieving legally coherent and socially sustainable outcomes in the digital creative economy.

Keywords

Transformative Use, AI-Generated Art, NFT Copyright, Fair Use Doctrine, Hybrid Authorship.

HOW TO CITE:

Chicago Manual of Style Footnote:

¹ Jeralyn Valencia, Fajar Sugianto, Atsuko Yamamoto, Jerry Shalmont, and Nadya Suryo, “Hybrid Authorship and Legal Uncertainty: Rethinking Intellectual Property for AI-Generated and NFT Art,” *Journal of Law and Legal Reform* 7, no 2 (2026): 987-1082, <https://doi.org/10.15294/jllr.v7i2.32504>.

Chicago Manual of Style for Reference:

Valencia, Jeralyn, Fajar Sugianto, Atsuko Yamamoto, Jerry Shalmont, and Nadya Suryo. “Hybrid Authorship and Legal Uncertainty: Rethinking Intellectual Property for AI-Generated and NFT Art.” *Journal of Law and Legal Reform* 7, no 2 (2026): 987-1082. <https://doi.org/10.15294/jllr.v7i2.32504>.

Introduction

The convergence of artificial intelligence (AI), blockchain technology, and non-fungible tokens (NFTs) is rapidly redrawing the boundaries of creative production, market participation, and legal protection. Despite this rapid market expansion, existing legal scholarship has largely treated NFTs either as technological artifacts or market phenomena, resulting in insufficient examination of the doctrinal consequences of hybrid human–AI authorship for copyright, contractual enforceability, and evidentiary attribution across jurisdictions¹. In the digital art sector, artificial intelligence is utilized in two primary ways: fully automated systems are capable of creating artworks without any human input, while hybrid approaches enable artists to use AI as a collaborative tool in the creative process.

Together, these innovations have produced a new genre of AI art that blends computational techniques with human creativity. AI-generated art is rapidly reshaping the landscape of NFT markets, moving from experimental novelty to a central force in digital culture. Recent industry forecasts, based on aggregated marketplace transaction data, trend analysis of AI-assisted minting activity, and predictive adoption models employed by prominent NFT analytics platforms, suggest that by the conclusion of 2025, AI-generated NFTs will generate over \$18 billion for global NFT marketplaces and constitute nearly 30% of all new digital collections.² The emergence of AI-generated art, as mapped by Du Sautoy, reveals a profound reconfiguration of creativity and authorship within the digital era. Rather than acting solely as a substitute for human ingenuity, artificial intelligence increasingly assumes the role of an active co-creator, a catalyst for symbiotic creativity where human artists and algorithms engage in a dynamic, iterative exchange.³

¹ Anastasiia Terekhova, “The Impact of AI-Generated NFT Art on the Global Art Market: Trends and Perspectives,” *Scientific Journal of Bielsko-Biala School of Finance and Law* 29, no. 1 SE-Articles (March 2025): 65, <https://doi.org/10.19192/wsfp.sj1.2025.8>

² NonFungible.com, *NFT Market Report 2023–2024: Trends, Segmentation, and Forecasts*, NonFungible Research, 2024.

³ Marcus du Sautoy, *The Creativity Code: How AI Is Learning to Write, Paint and Thinkd* (London: Fourth Estate, 2019), 212, see Chapter 15.

In the hybrid paradigm, artists leverage AI not merely as a passive instrument but as an imaginative interlocutor: algorithms suggest novel patterns, propose unexpected solutions, or generate raw material from which new artistic forms are selected, adapted, and imbued with human meaning.⁴ This dialogical partnership has created a “symbiotic creative environment” where new ideas can come up that neither humans nor machines could come up with on their own.⁵

In parallel, advances in deep learning have enabled the rise of fully automated generative systems algorithms capable of independently producing complex works by mining vast datasets of existing art and extrapolating them into forms that are simultaneously novel and referential. Projects such as *The Next Rembrandt* and the creation of Edmond Belamy exemplify this capacity for autonomous creativity, raising intricate questions about intention, agency, and legal authorship that continue to challenge established norms in the art world.⁶

Crucially, both hybrid and automated models have not only expanded the technical and aesthetic boundaries of digital art but have also disrupted market dynamics and institutional practices.⁷ Their proliferation has attracted the sustained attention of collectors, critics, and major cultural institutions, contributing to the exponential growth of a new digital art economy.⁸ Nowhere is this convergence of technology, art, and controversy more visible than in the international ascent of the robot artist Ai-Da. As documented by Lima, Ai-Da’s participation in headline events such as the Venice Biennale, the London Design Biennale, and parliamentary hearings at the UK House of Lords, combined with extensive global press coverage, has elevated her from a technological curiosity to a central and hotly debated figure within the contemporary art world.⁹ Her exhibitions and performances have not only catalyzed critical and institutional debate about authorship, value,

⁴ Sautoy, *The Creativity Code: How AI Is Learning to Write, Paint and Thinkd*.

⁵ Sautoy.

⁶ Sautoy.

⁷ Sautoy.

⁸ Sautoy.

⁹ Eleonora Lima, “AI Art and Public Literacy: The Miseducation of Ai-Da the Robot,” *AI and Ethics* 4, no. 3 (2024): 845, 850, <https://doi.org/10.1007/s43681-024-00488-5>.

and creative agency,¹⁰ but have also served as focal points for public discussions about the very legitimacy of algorithmic and robotic creation in art. Ai-Da's prominence illustrates how AI-driven practices, whether collaborative or independent, are now directly reshaping conceptions of originality, market value, and the evolving boundaries of creative legitimacy in the digital era.¹¹

The international prominence of the robot artist Ai-Da illustrates how AI-assisted and autonomous creative systems have moved from experimental novelty into mainstream artistic and institutional settings. While Ai-Da is not treated here as a legal case study, its reception underscores the growing tension between technological practice and legal frameworks still grounded in human-centered authorship. The relevance of such examples lies not in their cultural novelty but in how they expose the inadequacy of existing legal categories to address hybrid and automated forms of creativity.

The legal uncertainty surrounding AI-generated art is not uniform but varies significantly depending on the technical architecture of the system involved. Prompt-based systems, in which human users exercise creative control through iterative textual or visual instructions, raise questions primarily about the threshold of human authorship and the scope of protectable expression. By contrast, works generated through generative adversarial networks or diffusion models pose deeper challenges related to originality, attribution, and potential infringement from the training data, as these outputs come from autonomous statistical processes trained on large datasets. Fully automated systems, operating with minimal or no human intervention, further complicate traditional doctrines by destabilizing the assumed link between creative intent and legal authorship. These technical distinctions are legally consequential, as they require differentiated regulatory responses rather than a single, undifferentiated characterization of AI-generated art as occupying a "gray zone."

However, at precisely the moment when these technologies promise to democratize access and distribute opportunity, a deeper and more intractable set of problems comes into view. The basic doctrines of

¹⁰ Lima, "AI Art and Public Literacy: The Miseducation of Ai-Da the Robot."

¹¹ Lima.

copyright and intellectual property law developed for a world of human authors, physical media, and territorial markets now strain to accommodate collaborative, distributed, and code-driven modes of creation.¹² The very notion of “authorship” itself has become contested and contingent: who deserves credit or control when a work is shaped as much by data, prompts, and algorithms as by human hand?¹³ In an era of infinite remix and AI augmentation, what defines originality or creative labor?¹⁴ These uncertainties are amplified by the broader disruptions triggered by crypto art and NFTs, which have created new forms of scarcity and value around digital objects yet also generated criticism regarding speculation, fraud, and the possible creation of economic bubbles within the art market.¹⁵

Recent studies indicate that the exponential growth of NFT transactions, with market turnover reaching over \$40 billion in 2021 alone and tens of millions of transactions globally, has been accompanied by intense debate over whether this surge truly democratizes the art world or instead fuels instability and deepens inequalities among participants.¹⁶ Moreover, while NFT-based digital art and crypto art are often celebrated as engines of creative and economic empowerment, their technical architecture frequently sidelines traditional legal safeguards such as automatic royalties, clear provenance, and enforceable IP rights in favor of algorithmic certificates of authenticity that may not always correspond to real-world control over creative outputs.¹⁷

Legal responses, so far, have been fragmented and reactive. In the United States, courts and the Copyright Office enforce a strict human-authorship requirement, routinely excluding even sophisticated hybrid works from protection and leaving vast swathes of innovation in

¹² Patrici Calvo, “Cryptoart: Ethical Challenges of the NFT Revolution,” *Humanities and Social Sciences Communications* 11, no. 1 (2024): 2–4, <https://doi.org/10.1057/s41599-024-02872-2>.

¹³ Calvo, “Cryptoart: Ethical Challenges of the NFT Revolution.”

¹⁴ Calvo.

¹⁵ Calvo.

¹⁶ Chainalysis Team, “NFT Transaction Activity Stabilizing in 2022 After Explosive Growth in 2021,” Chainalysis, 2022.

¹⁷ Chainalysis Team.

doctrinal limbo.¹⁸ The European Union, while notionally more flexible, grounds copyright in the “author’s own intellectual creation,” with little clarity for mixed human–AI works.¹⁹ In China, although there are no binding judicial precedents systematically governing copyright infringement claims involving AI training, courts have begun substantively addressing the copyright ability of AI-generated content (AIGC). Notably, in November 2023, the Beijing Internet Court ruled in the country’s first AI-generated image copyright case that such content can qualify as a protected “work” under copyright law, provided it reflects the original intellectual input of a human creator and the potential liability of generative AI service providers.²⁰ Meanwhile, NFT marketplaces and platforms have largely deferred to general intellectual property norms, focusing on anti-plagiarism and fraud detection rather than establishing explicit rules on authorship or ownership of AI-generated and hybrid works. For instance, Open Sea relies on a DMCA-style takedown mechanism to handle copyright or trademark violations without offering any guidance specific to AI-generated content,²¹ while Super Rare prohibits falsified authorship under its Terms of Service but does not address AI-assisted creation. At the same time, platforms like Open Sea, Rarible, and Looks Rare are increasingly integrating AI tools for smart curation, metadata tagging, and predictive market analytics. However, despite these technological advances, their policies still lack legal clarity regarding whether AI-assisted outputs qualify for copyright protection or valid claims of authorship.²²

This institutional lag has made the gap between the realities of creative practice and the guarantees of law even bigger. Most creators and buyers in the NFT ecosystem do not benefit from legal certainty but must navigate a patchwork of platform policies, fragmented national

¹⁸ Copyright.gov, “Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence” (2023).

¹⁹ Official Journal of the European, “Regulation (EU) 2024/1689 on Harmonised Rules on Artificial Intelligence (AI Act), Pub. L. 2024/1689, Union,” 2024.

²⁰ AWAPoint, “China’s First AI-Generated Picture Copyright Infringement Case: Legal Implications,” 2024.

²¹ OpenSea Help Center, “OpenSea Help Center,” 2024.

²² BlockchainTechs.io, “How AI Generated NFT Art Is Shaping the Future of NFT Art Collections,” 2025.

rules, and code-based agreements whose enforceability remains unclear. Empirical studies and industry reports indicate that the majority of disputes over authorship, royalties, or infringement are settled, if at all, through private negotiation or intervention by NFT platforms rather than through formal legal proceedings or automated smart contract execution.²³ In practice, rights and remedies are determined less by the substance of creative contribution than by the jurisdictional quirks of law, the technical architecture of smart contracts, or the discretionary policies of dominant marketplaces.²⁴

What emerges is a global legal “gray zone,” in which access to recognition, reward, or justice is as likely to depend on technical sophistication or forum selection as on the merits of the creative work itself. Fragmented governance allows for regulatory arbitrage and deepens the divide between well-resourced, technologically savvy actors and the majority of creators, especially those in the Global South or from marginalized communities who remain exposed to uncertainty and exclusion.²⁵

Thus, the central challenge is not simply one of law “catching up” to technology, but of reimagining legal, institutional, and technical frameworks for a digital creative economy that is plural, dynamic, and unevenly resourced. Can established regimes adapt to secure rights, incentivize innovation, and distribute value fairly in the age of hybrid authorship and on-chain markets? Or does the persistence of legal gray zones and technical patchworks signal a more fundamental need for transformation for new forms of adaptive, just, and inclusive governance?

To address these questions, this analysis pursues two core objectives: first, to map the doctrinal, empirical, and structural dilemmas

²³ Cemre Ç. Kadioglu Kumtepe, *Defining Boundaries of Due Process in Blockchain Arbitration* (Radboud University Press, 2025), 43, https://doi.org/10.54195/FMVV7173_CH02.

²⁴ Andres Guadamuz, “The Treachery of Images: Non-Fungible Tokens and Copyright,” *Journal of Intellectual Property Law & Practice* 16, no. 12 (December 2021): 6–7, <https://doi.org/10.1093/jiplp/jpab152>.

²⁵ OECD/KDI, *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses* (Paris: OECD Publishing, 2021), <https://doi.org/10.1787/8fa190b5-en>.

posed by partial AI authorship and blockchain-enabled art; second, to interrogate how divergent regimes in the U.S., EU, and Asia shape incentives, access, and risk for creators and platforms, as well as to evaluate whether technical solutions like programmable rights, smart contracts, and blockchain evidence can close the enforcement and equity gaps, or whether new forms of legal and institutional innovation are required.

At stake is not only the fate of digital art or the refinement of legal doctrine, but the foundational terms by which creative agency, recognition, and economic participation will be distributed in the next era of cultural and economic life.

This article adopts a normative juridical and comparative doctrinal methodology. Its main goal is to look at how current copyright and digital asset laws deal with the rise of AI-generated and hybrid creative works. References to market data, NFT platform practices, and industry reports serve a contextual function: they illustrate the real-world implications of doctrinal fragmentation and regulatory uncertainty, rather than constituting independent empirical testing.

The analysis assesses competing legal approaches against three normative benchmarks relevant to law reform: legal certainty in authorship and protectability, institutional enforceability of rights across jurisdictions, and distributive fairness in access to digital creative markets. These criteria guide the comparative evaluation and inform the reform-oriented conclusions advanced in the final section.

This article employs a normative juridical method, combining doctrinal and comparative legal analysis with targeted empirical review.²⁶ For the purposes of this study, targeted empirical review refers to the selective use of market analytics and technical literature chosen on the basis of relevance to authorship disputes and enforceability of rights in AI-assisted NFT markets. The study systematically examines national statutes, international agreements, regulatory guidelines, and landmark judicial decisions governing copyright, blockchain, and smart contract

²⁶ Ade Adhari, Fransisca Iriani Roesmala Dewi, Anis Widyawati, Darius Andana Haris, and Dwiky Chandra. 2025. "Rehabilitation through Reading: Evaluating Prisoners' Right to Literacy As a Tool to Reduce Recidivism". *Indonesian Journal of Criminal Law Studies* 10 (2): 644. <https://doi.org/10.15294/ijcls.v10i2.29687>.

law in the United States, European Union, China, Japan, Singapore, Vietnam, and Thailand. Core legal sources include the U.S. Copyright Act, the Berne Convention, the EU InfoSoc Directive, and relevant national laws on electronic signatures, digital evidence, and AI governance. Case law analyzed includes *Feist*, *Thaler v. Perlmutter*, *Infopaq*, *Levola*, *Painer*, *Zarya of the Dawn*, *Kashtanova*, and *Li v. Liu*. Comparative evaluation is informed by policy documents from WIPO, OECD, and UNESCO, platform guidelines from leading NFT marketplaces (OpenSea, SuperRare, Async Art), and empirical market data from NFTGo and NonFungible.com. Theoretical frameworks such as originality doctrine, transformative use, and fair use are integrated with perspectives from law and economics and critical legal studies. The research is limited by the evolving nature of both technology and regulation, as well as the variability in national implementation and enforcement. No fieldwork or direct interviews were conducted; the analysis is based entirely on published legal materials, case law, policy reports, and technical/industry literature. As a result, the analysis does not purport to offer an empirical assessment of on-the-ground implementation or institutional practice, and the findings should be understood as analytically generalizable at the doctrinal and regulatory level rather than as predictive of enforcement outcomes in specific jurisdictions.

Rather than proposing reform in abstract or technologically deterministic terms, this article derives its reform orientation from a normative evaluation of existing legal frameworks. The comparative analysis that follows does not seek to rank jurisdictions or identify a single optimal model but to examine how different regulatory choices shape legal certainty, enforceability of rights, and distributive outcomes in markets increasingly defined by human–AI collaboration. By identifying recurring structural tensions across jurisdictions, the analysis aims to clarify where legal adaptation is necessary to preserve the coherence and legitimacy of intellectual property law under conditions of technological transformation.

A. Doctrinal Foundations and Comparative Law: The Crisis of Partial AI Authorship and Originality

The doctrine of authorship in copyright law has never been a static or value-neutral principle; rather, it has evolved in response to changing historical, economic, and cultural imperatives. From the enactment of the Statute of Anne in 1710 to the internationalization of copyright through the Berne Convention in 1886, the legal figure of the solitary, original author did not emerge organically but was instead deliberately constructed to serve specific institutional and economic interests. This construct was not a neutral or universal legal archetype; it was strategically designed to address concerns regarding cultural authority, profit control, and the legitimacy of creative ownership in the era of mechanical reproduction. It reflected a shift from collective modes of authorship toward individual proprietary claims, reinforcing a commodified understanding of creative labour that aligned with the expanding market logic of modern capitalism.²⁷

The modern concept of the author as an “originator” vested with exclusive legal rights was never a natural or inevitable construct, but rather a strategic legal fiction shaped by the demands of the market economy. As demonstrated by Martha Woodmansee and Mark Rose, this notion of authorship emerged in the 18th century to legitimize the commodification of creative labor, justify proprietary control over intangible outputs, and stabilize transactions in an increasingly expansive publishing industry.²⁸ foundational studies reveal that what we now treat as doctrinal originality was historically mobilized to rationalize the allocation of exclusive rights not on account of intrinsic creative merit, but as a juridical solution to economic anxieties over control, value, and

²⁷ World Intellectual Property Organization, *Overview of the International Protection of Copyright and Related Rights: From the Berne Convention to the WIPO Copyright Treaty (WIPO/CR/DAM/05/8)* (Geneva: World Intellectual Property Organization, 2025), 4–5.

²⁸ Martha Woodmansee, “The Genius and the Copyright: Economic and Legal Conditions of the Emergence of the ‘Author,’” *Eighteenth-Century Studies* 17, no. 4 (August 1984): 429–31; 6–12, <https://doi.org/10.2307/2738129>.

access in an age of mass reproduction.²⁹ Yet, as Woodmansee and Rose have shown, this foundational vision of authorship has always been historically contingent and therefore unstable.³⁰

Recognizing authorship as a historically contingent legal construct does not require dismantling the incentive structure of copyright law. Rather, it permits a more precise calibration of authorship criteria in response to changing creative practices. In the context of AI-assisted creation, the argument suggests a shift from a binary inquiry into human versus machine authorship toward an assessment of human creative control. When a human actor makes meaningful decisions about prompt design, choosing between generated outputs, iterative refinement, or aesthetic curation, authorship can stay firmly rooted in human agency without giving the AI system legal personality. Such a control- and selection-based approach preserves the economic and normative foundations of copyright while acknowledging that creativity increasingly unfolds through human–machine collaboration rather than solitary authorship.

Read together, these theoretical accounts do not merely historicize authorship but provide concrete guidance for contemporary doctrinal reform. If authorship is viewed as a functional legal construct rather than a metaphysical assertion regarding creativity, then AI-authorship doctrines ought to be realigned to focus on discernible aspects of human creative judgment rather than the outright prohibition of technological assistance. This implies reform directions that prioritize human control, selection, and curatorial decision-making as the basis for protection, while withholding copyright from outputs generated through fully autonomous systems without meaningful human intervention. In this way, historical theory informs a reform agenda that preserves incentive structures without extending authorship to machines.

It has consistently been challenged by the inherently collective and collaborative nature of creative production, which the sole-author paradigm fails to accommodate.³¹ These tensions have only intensified

²⁹ Woodmansee, “The Genius and the Copyright: Economic and Legal Conditions of the Emergence of the ‘Author.’”

³⁰ Woodmansee.

³¹ Mark Rose, *Authors and Owners: The Invention of Copyright* (Cambridge, MA: Harvard University Press, 1993), 47–46, <https://doi.org/10.2307/3117041>.

with successive waves of technological disruption from photography and phonography to digital sampling and algorithmic generation, which have exposed the structural limits of a human-centered model. Copyright systems persist in reinforcing the importance of “originality” and “human intent,” despite ongoing legal adaptations that redefine these concepts.

Lawrence Lessig, in his influential work *Code and Other Laws of Cyberspace*, argues that in the digital age, “code” the software and hardware architectures that structure cyberspace, acts as a primary regulator of behavior, shaping rights and constraints as directly as, or even more powerfully than, legal statutes. He explains:

*“And finally, an analog for architecture regulates behavior in cyberspace code. The software and hardware that make cyberspace what it is constitute a set of constraints on how you can behave. The substance of these constraints may vary, but they are experienced as conditions on your access to cyberspace... These are features selected by code writers; they constrain some behavior by making other behavior possible, or impossible.”*³²

Lessig further emphasizes that “the code of cyberspace is becoming just another tool of state regulation. Indirectly, by regulating code writing, the government can achieve regulatory ends, often without suffering the political consequences that the same ends, pursued directly, would yield.”³³ The core insight is that those who design and control code now including designers of AI algorithms and platforms -- effectively determine the boundaries of digital rights, participation, and exclusion.³⁴ As digital technologies evolve, this architectural power is not static, but continually constructed and reconstructed to reflect (or contest) underlying values and interests.³⁵

In contemporary contexts, this theoretical framework applies directly to AI: algorithmic systems and automated architectures much

³² Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).

³³ Lessig.

³⁴ Lessig.

³⁵ Lessig.

like the code of early cyberspace now embed rules that determine authorship, access, and legal status, often outside the reach of traditional law.³⁶ Thus, Lessig's insight remains acutely relevant: as society entrusts ever more governance to code, the central question is not only "what does the law say?" but "who writes the code, and whose values does it serve?"

These tensions have reached a critical juncture in the twenty-first century, as creativity at the intersection of artificial intelligence (AI), non-fungible tokens (NFTs), and digital platforms has profoundly destabilized traditional categories of authorship. The emergence of the "partial AI author", a human creator whose agency is interwoven with machine intelligence, renders the conventional boundary between author and tool obsolete. As Denis Yi Tenen argues, the contemporary notion of authorship is undergoing a radical shift: no longer rooted in a singular, sovereign figure, but instead emerging as a distributed system of human, institutional, and algorithmic agents.³⁷ Authorship today is shaped by modular contributions, collaborative infrastructures, and automated systems, where agency is fragmented and dynamically negotiated. AI-assisted creation particularly highlights this model, as it blurs the boundaries between creator, tool, and platform. In such contexts, authorship is not a static legal status but a fluid assemblage of responsibilities and constraints embedded in sociotechnical networks.³⁸ In today's NFT-driven art market, legal status hinges not only on the originality of expression but increasingly on the provenance and degree of human-machine collaboration. By 2024, AI-generated NFTs accounted for over 62% of total global NFT sales, demonstrating that machine-assisted creative processes now dominate the digital art market.³⁹

³⁶ Lessig.

³⁷ Dennis Yi Tenen, "Author—Anonymous and Distributed," *New Techno-Humanities* 4, no. 1 (2024): 54–56, <https://doi.org/10.1016/j.techum.2024.07.001>.

³⁸ Yi Tenen, "Author—Anonymous and Distributed."

³⁹ Anastasiia Terekhova, "The Impact of AI-Generated NFT Art on the Global Art Market: Trends and Perspectives," *Scientific Journal of Bielsko-Biala School of Finance and Law* 29, no. 1 SE-Articles (March 2025): 65, <https://doi.org/10.19192/wsfip.sj1.2025.8>.

Table 1. AI NFT Sales and Market Volume, 2020–2024 (Descriptive Market Indicators).

Year	Total NFT Sales (\$M)	AI NFT Sales (\$M)	Share of NFT	R^2
2020	150	10	6.7%	0.75
2021	250	50	20%	0.80
2022	400	150	37.5%	0.85
2023	600	300	50%	0.88
2024	800	500	62.5%	0.90

Sources: Anastasiia Terekhova, “The Impact of AI-Generated NFT Art on the Global Art Market: Trends and Perspectives,” ASEJ, Vol. 8, No. 1 (2024): 64.

Note: The R^2 values reported in this table reflect descriptive goodness-of-fit measures derived from simple linear trend visualization of aggregated market data. They are included solely to illustrate directional consistency over time and do not represent inferential regression analysis, causal modeling, or variable correlation.

The increasing role of AI augmentation and hybrid creative workflows challenges traditional legal notions of authorship and originality, especially as most of these works remain unrecognized under conventional copyright frameworks.⁴⁰ This legal lag produces uncertainty and weakens incentive structures in the most innovative segments of the market, precisely where dynamic experimentation thrives.⁴¹

Building on this breakdown of traditional authorship, the technical foundations of generative AI further expose the growing incompatibility between copyright’s doctrinal categories and the actual processes of model development. The industrial-scale ingestion of copyrighted content, often without consent, lies at the heart of this disruption. Leading AI firms like OpenAI and Anthropic have asserted

⁴⁰ Terekhova, “The Impact of AI-Generated NFT Art on the Global Art Market: Trends and Perspectives.”

⁴¹ Terekhova.

that it would be “impossible” to develop high-performing models without sweeping up massive volumes of online materials, many of which are protected by copyright, due to the sheer scale, diversity, and linguistic nuance required to train models capable of generalizing across domains.⁴²

The technical evolution of generative artificial intelligence (GenAI) is inseparable from the architecture of its training data. Modern models, most notably diffusion models, large language models (LLMs), and generative adversarial networks (GANs) are engineered to process and synthesize vast and highly heterogeneous datasets, comprising not only natural language and images but also code, audio, and a range of other modalities. This diversity enables GenAI systems to identify deep statistical patterns, capture complex semantic relationships, and ultimately generate creative outputs, whether text, images, or other media, that can rival or even surpass traditional human production in both scope and complexity.⁴³ The purpose is not merely to “memorize” information but to extract complex patterns, semantic relationships, and probabilistic rules that allow the system to generate contextually relevant and often highly creative outputs. This capability underpins advances in everything from AI-generated text and code (LLMs) to high-resolution synthetic images (diffusion and GAN models) and extends to the automated production of original works in visual arts, music, scientific discovery, and other domains of content creation.⁴⁴ In this way, GenAI is transforming not only the creative industries but also fields such as research, education, and automated knowledge work.

The assembly of these massive datasets is itself a defining feature of GenAI’s contemporary trajectory. Standard industry practice overwhelmingly relies on automated web scraping and large-scale data mining to harvest content from across the internet, academic repositories, digital archives, and even proprietary platforms. While some

⁴² Nitasha Tiku, “New Research Shows It’s Possible to Build Powerful AI without Violating Copyright - The Washington Post,” 2025.

⁴³ World Intellectual Property Organization, Patent Landscape Report: Generative Artificial Intelligence (Geneva, issued 2024), 24–26, <https://doi.org/10.34667/tind.49740>.

⁴⁴ World Intellectual Property Organization, Patent Landscape Report: Generative Artificial Intelligence.

limited efforts are made to license or curate specific datasets for proprietary or sensitive applications, the norm is aggregation without granular record-keeping regarding data origin, copyright status, or permissions.⁴⁵ As a result, the provenance of training data is typically opaque, with public domain, open-access, and copyrighted materials commingled in ways that undermine traceability and complicate both compliance and auditing.

Generative models such as GANs and diffusion models produce images by learning complex data patterns and then synthesizing new content that mimics those patterns. Diffusion models, for example, begin with random noise and iteratively “denoise” it, guided by the neural network, to produce photorealistic images, while GANs use a generator-discriminator framework to improve image realism over time. This process is data-driven: the more varied and expansive the training set, the more nuanced and creative the outputs; hence, the relentless industry pursuit of larger and more diverse datasets.⁴⁶

While modern generative AI models have the technical capacity to closely replicate, remix, or adapt protected works, the risk of copyright infringement is not uniform across all systems. The core distinction lies in the origin and governance of their training data. Public domain data refers to information such as digitized government records, historical archives, and open-source materials—that is legally available for unrestricted use by anyone. Many general-purpose AI models are trained on vast amounts of such publicly accessible data, often collected from the internet, open repositories, and large-scale web crawls. However, not all publicly sourced data is truly free of copyright or other restrictions; the ambiguous or mixed legal status of online content means that unauthorized use of protected works can easily occur during model training, creating a heightened risk of copyright infringement, data leakage, and compliance failures. In contrast, private domain data comprises proprietary, confidential, or enterprise-owned information, including internal documents, business records, and customer datasets, all maintained within a closed and controlled environment. AI systems that operate on private domain data give organizations the ability to

⁴⁵ World Intellectual Property Organization.

⁴⁶ World Intellectual Property Organization.

govern exactly how their data is processed, secured, and used; implement robust compliance protocols; and ensure that all inputs are fully vetted for legal and ethical standards.⁴⁷ This level of control significantly reduces exposure to copyright liability and regulatory risk, as both the provenance and usage of training data are subject to direct oversight. Ultimately, the distinction between public and private domain data is not merely technical or academic but fundamental to understanding and managing the varying degrees of legal and ethical risk faced by generative AI. Systems built on uncontrolled or insufficiently documented public data sources are inherently more vulnerable to legal challenges, whereas those based on private, well-governed datasets can better enforce provenance, consent, and compliance at every stage of development and deployment.⁴⁸

Projects like Common Corpus and KL3M provide concrete, fully documented examples of a “copyright-clean” approach to large-scale LLM data collection and training. Unlike conventional web-scraped datasets, both projects are explicitly designed to eliminate copyright and contract risk at the source, setting a new technical and ethical benchmark for lawful, reproducible AI development. Common Corpus is the largest open-source, multi-lingual dataset constructed entirely from public domain and permissively licensed content, meticulously filtered to ensure every token is legally auditable and suitable for use in regulated jurisdictions such as the EU.⁴⁹ KL3M, in turn, introduces a formal three-test protocol for data inclusion only selecting documents that are (1) free from copyright at creation, (2) entered into the public domain, or (3) under sufficiently unencumbered license, with full metadata and provenance traceability for every artifact.⁵⁰

⁴⁷ Indah Sri Utari et al., “The Digital Sanctuary: Forging Legal And Ethical Frameworks For Interfaith Coexistence Online,” *Contemporary Issues on Interfaith Law and Society* 4, no. 2 (2025), <https://doi.org/10.15294/ciils.v4i2.35309>.

⁴⁸ AI21 Labs, “Private AI vs. Public AI: What Is the Difference?,” AI21, 2025.

⁴⁹ Pierre-Carl Langlais et al., “Common Corpus: The Largest Collection of Ethical Data for LLM Pre-Training,” *ArXiv Preprint ArXiv:2506.01732*, 2025.

⁵⁰ Michael J Bommarito, Jillian Bommarito, and Daniel Martin Katz, “The KL3M Data Project: Copyright-Clean Training Resources for Large Language Models,” 2025.

The existence and design of these projects address several persistent industry critiques: first, they prove that it is technically possible to construct LLM training data pipelines that are legally defensible, fully transparent, and auditable at scale.⁵¹ Second, they empirically demonstrate the magnitude of manual curation, ongoing licensing review, and domain expertise required to reach this level of compliance.⁵² Common Corpus, for example, required the development of dedicated cleaning and filtering pipelines, and KL3M's protocol results in the systematic exclusion of any material with attribution, non-commercial, or share-alike restrictions, drastically reducing the risk profile but at the expense of dataset diversity and scalability.⁵³

Despite their significance, both projects also reveal inherent trade-offs: The intense resource investment ranging from legal review to document-level filtering and format normalization makes it difficult for these “gold standard” datasets to match the sheer scale, topical diversity, and linguistic variety of conventional web-crawled corpora used by most commercial models.⁵⁴ As a result, while Common Corpus and KL3M set the highest bar for compliance and auditability, they remain more suitable for domains and organizations where legal certainty, transparency, and reproducibility are critical, rather than for rapid, broad-market AI deployment.⁵⁵

By contrast, commercial AI development predominantly relies on proprietary or mixed (often unlicensed) datasets, which may include copyrighted web content, private user data, or domain-specific internal corporation data.⁵⁶ While this strategy accelerates deployment, reduces upfront costs, and enables higher accuracy and flexibility across general and specialized tasks, it also exposes developers and users to increased

⁵¹ Langlais et al., “Common Corpus: The Largest Collection of Ethical Data for LLM Pre-Training.”

⁵² Langlais et al.

⁵³ Langlais et al.

⁵⁴ Langlais et al.

⁵⁵ Langlais et al.

⁵⁶ European Union Intellectual Property Office (EUIPO), *The Development of Generative Artificial Intelligence from a Copyright Perspective* (European Union Intellectual Property Office, 2025), 130–31, 169, <https://doi.org/10.2814/3893780>.

legal and regulatory risk, opaque data practices, and diminished control over compliance and transparency.⁵⁷ Public AI systems such as ChatGPT, Gemini, or Copilot are designed for mass adoption, prioritizing convenience, scalability, and rapid experimentation, but typically operate as ‘black boxes’ with limited user control over data processing, retention, or model behaviour.⁵⁸ Data is processed externally, and user inputs may be retained or reused, raising concerns about privacy, data leakage, and competitive exposure.⁵⁹ Conversely, private AI deployed on-premise or in secure private clouds using proprietary data offers full operational control, strict data governance, tailored compliance, and domain-specific customization but requires significant investment in infrastructure, expertise, and ongoing management.⁶⁰

Thus, the choice between public-domain-based and private/proprietary-data-based AI is not a trivial one but a strategic decision that affects cost structure, compliance posture, security profile, scalability, and the ability to support critical, regulated, or high-value applications. The scalability and resource intensity of lawful, transparent public-domain models have so far limited their widespread adoption, especially among commercial providers seeking rapid technical progress. As a result, most leading commercial models, including OpenAI’s GPT series and Anthropic’s Claude, continue to rely on expedient ingestion of web-scraped, often unlicensed content, prioritizing speed and coverage at the expense of provenance, transparency, and legal certainty.⁶¹

This paradigm introduces cascading risks and opacity, particularly for sectors where provenance, compliance, and auditability are paramount, and underscores the urgent need for enforceable standards in data governance, accountability, and transparency throughout the AI lifecycle.

As synthesized from the industry summary and discussion on governance risks provided in WIPO’s patent landscape report, the divergence between these two data paradigms - one privileging legality

⁵⁷ European Union Intellectual Property Office (EUIPO), *The Development of Generative Artificial Intelligence from a Copyright Perspective*.

⁵⁸ European Union Intellectual Property Office (EUIPO).

⁵⁹ European Union Intellectual Property Office (EUIPO).

⁶⁰ European Union Intellectual Property Office (EUIPO).

⁶¹ European Union Intellectual Property Office (EUIPO).

and transparency, the other prioritizing speed and competitive advantage - underscores the urgent need for enforceable data provenance standards, comprehensive audit mechanisms, and adaptive legal doctrines capable of separating good-faith machine learning from extractive, rights-disregarding practices. Without such frameworks, the continued reliance on opaque and mixed data sources will remain a critical point of vulnerability for both the GenAI industry and the evolving architecture of copyright law.⁶²

This doctrinal tension is perhaps most pronounced in the United States, where the insistence on “human authorship” remains a foundational legal barrier, rigorously enforced by both courts and administrative agencies amid growing technological disruption. The Supreme Court’s foundational decision in *Feist Publications, Inc. v. Rural Telephone Service Co.* (1991) cemented “originality” as a touchstone of copyright, defined by “independent creation” and a “modicum of creativity” traceable to a natural person.⁶³ In practice, this anthropocentric baseline has guided not only judicial reasoning but also the entire architecture of U.S. copyright registration and enforcement.

The contemporary crisis was brought into sharp relief by *Thaler v. Perlmutter* (D.D.C. 2023), where the court faced a work generated wholly by AI without human creative intervention. The court’s ruling was categorical: “Only works created by human beings are entitled to copyright protection under U.S. law.”⁶⁴ This was no mere technicality; the court engaged directly with both statutory language and policy rationales, expressing concern that extending authorship to AI systems would undermine the incentive structure and moral underpinnings of copyright.⁶⁵ The decision tracked the U.S. Copyright Office’s evolving administrative guidance, which, since 2022, has required applicants to

⁶² World Intellectual Property Organization, Patent Landscape Report: Generative Artificial Intelligence.

⁶³ *Feist Publications Inc, “Rural Tel. Serv. Co.,”* 1991.

⁶⁴ *Thaler v. Perlmutter*, “United States District Court for the District of Columbia: Memorandum Opinion,” 2023.

⁶⁵ *Perlmutter*.

explicitly disclose and separate any AI-generated content, registering only the “human-authored” portions of a hybrid work.⁶⁶

The 2023 guidance further clarifies that copyright registration will be refused for material generated autonomously by AI, regardless of its artistic or economic value. Applicants are required not only to disclose the use of AI but also to delineate the specific portions created by human authorship and explain the nature of the human author’s “creative control” over the final expression. This procedural requirement has effectively narrowed the scope of registrable content for hybrid works, especially in NFT and generative art markets where algorithmic contribution is often substantial. In many cases, applicants are asked to disclaim non-human elements or respond to further inquiries from the Copyright Office, a process that can delay registration or result in partial refusals. Consequently, creators are left with critical parts of their work unprotected under copyright, prompting increased reliance on smart contracts, private licensing arrangements, and blockchain verification tools as alternative mechanisms to safeguard economic and reputational interests.⁶⁷

Based on the WIPO Patent Landscape Report, the resulting economic and creative fallout is stark. Creators operating at the intersection of AI and art face persistent doctrinal uncertainty, including the risk of orphaned works, the inability to license or collect royalties, and structural gaps in enforcing provenance and authorship. Despite the U.S. leading global NFT sales and generative art innovation, its legal framework remains deeply fragmented, with courts and agencies reluctant to extend copyright to AI-generated works. As a result, creators must increasingly rely on contractual proxies such as smart contracts embedded in NFT metadata or marketplace terms of service to assert and manage their rights. Yet these mechanisms often lack transparency, standardization, and legal enforceability, especially across jurisdictions, leaving creators vulnerable to exploitation and revenue loss despite

⁶⁶ Copyright.gov, Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence.

⁶⁷ Copyright.gov.

producing some of the most culturally and technologically significant digital assets of the current era.⁶⁸

The United States, despite being a global leader in generative technologies and NFT innovation, increasingly faces structural risks due to regulatory rigidity. As highlighted by recent analysis of cross-border tax and regulatory behaviour, America's domestic legal environment has become so complex and inflexible that it incentivizes companies to relocate assets, intellectual property, and entire business operations to more permissive jurisdictions. This form of large-scale regulatory arbitrage exemplified by U.S. insurers shifting over \$600 billion in life insurance reserves to Bermuda or pharmaceutical giants booking the majority of their profits offshore—reflects not only a tax challenge but also a deeper failure to legally adapt to global economic realities. If innovation in AI, digital assets, and IP enforcement continues to be governed by outdated or overly territorial doctrines, the U.S. risks eroding its own competitive advantage. Legal inflexibility not only drives capital flight and offshoring but also deters creative industries and digital entrepreneurs from relying on statutory protections, forcing them to rely on private contracts, technical measures, or foreign regimes to secure their rights. In effect, America's inability to evolve its regulatory architecture may undermine both domestic innovation ecosystems and its global leadership in the digital economy.⁶⁹

While critics argue that copyright's exclusion of AI-generated works reflects a failure to adapt to emerging creative processes, others defend this exclusion as essential. As Ginsburg notes, the legitimacy and symbolic coherence of copyright rest on its tether to human authorship — what she terms “authorial anchors.” From this perspective, even as non-human outputs command market attention, the core social bargain of copyright law grounded in human creativity and moral agency must remain intact to preserve public trust and normative coherence.⁷⁰

⁶⁸ World Intellectual Property Organization, *WIPO Scoping Study on IP Enforcement in Digital Creative Markets* (Geneva, 2024), 76–78.

⁶⁹ Felix Martin, “Why ‘America First’ Could End the Age of Arbitrage,” Reuters, 2025.

⁷⁰ Jane C Ginsburg, “Fifty Years of U.S. Copyright: Toward a Law of Authors’ Rights?,” 2022, 22.

A central question in the legal treatment of AI-generated and hybrid works concerns whether the use of copyrighted materials, either as training data or embedded creative components, can be justified under the doctrine of fair use. This inquiry is particularly salient given the large-scale, often non-consensual scraping of protected content by generative models. Under Section 107 of the U.S. Copyright Act, courts apply a four-factor balancing test to assess fair use, which considers: (1) the purpose and character of the use, including whether it is commercial or transformative in nature; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used; and (4) the effect of the use on the potential market for or value of the original. Among these, the first factor, “the purpose and character of the use,” has emerged as the most determinative in modern jurisprudence, especially when assessing whether the new work adds something sufficiently transformative to justify its use without permission.⁷¹

In the context of AI-generated outputs and NFTs, this factor becomes especially complex. Courts may examine whether the AI’s output meaningfully alters the original input’s expression, purpose, or function, for example, by translating text into visual formats, changing stylistic approaches, or generating outputs for commentary, education, or parody. However, when the underlying data includes copyrighted works from private domains, such as professional illustrations, music, or photography, without license or attribution, the fair use defense becomes more tenuous.⁷² In such cases, courts are likely to scrutinize both the commercial intent of the resulting product (such as monetized NFTs) and the market displacement risk posed to original creators. Thus, while transformation remains a cornerstone of the fair use analysis, its application to AI systems remains unsettled and heavily fact-dependent.⁷³

⁷¹ Legal Information Institute, “17 U.S. Code § 107 - Limitations on Exclusive Rights: Fair Use,” 1990.

⁷² Kenneth Bradley Sajogo, Fajar Sugianto, and Atsuko Yamamoto, “Comparative Analysis Regarding the Copyright Law on AI-Generated Art Between Indonesian and the United States: Unpacking Indonesian Legal Framework Conundrum,” *Jurnal Hukum Bisnis Bonum Commune* 8, no. 2 (August 2025): 213–242, <https://doi.org/10.30996/jhbbc.v8i2.12883>

⁷³ Caitlynn Nadya Aurelia, Velliana Tanaya, Fajar Sugianto, and Atsuko Yamamoto, “Enhancing Fair Use in Protecting Appropriated Artworks: A Comparative

In contrast to the United States' rigid authorial doctrine, the European Union adopts a more process-oriented conception of authorship—yet one that remains firmly grounded in anthropocentric principles. The foundational standard of “the author’s own intellectual creation” has been developed exclusively through the jurisprudence of the Court of Justice of the European Union (CJEU). In *Infopaq International A/S v Danske Dagblades Forening* (Case C-5/08), the CJEU established that copyright protection under EU law arises only when the subject matter is “the author’s own intellectual creation.” This criterion, now recognized as the EU standard for originality, requires that a work reflect the author’s free and creative choices and bears the stamp of their personal expression.

Read in the context of AI-assisted creation, *Infopaq* offers a more operational test than is often assumed. The emphasis on “free and creative choices” suggests that originality may subsist where a human actor meaningfully shapes the expressive outcome of an AI-assisted process, for example, through deliberate prompt construction, selective iteration, or curatorial judgment over generated outputs. What *Infopaq* excludes is not technological assistance as such, but expression that is mechanically produced without scope for human intellectual discretion. At the same time, the case exposes a structural limitation: where AI systems generate content autonomously, without identifiable moments of human choice, the *Infopaq* standard offers no clear basis for protection under existing EU law. Even brief extracts as short as 11 words can qualify as protected if they convey elements that express such intellectual creation. This judgment not only harmonized the originality threshold across EU directives (e.g., for software, databases, and photographs) but also affirmed that originality must be assessed autonomously under EU law, independent of national doctrines.⁷⁴

In *Eva-Maria Painer v Standard VerlagsGmbH and Others* (Case C-145/10), the CJEU affirmed that a portrait photograph qualifies for copyright protection under EU law when it constitutes the author’s own

Analysis of Safeguarding Indonesian Copyright Law,” *Lex Scientia Law Review* 9, no. 1 (2025): 1181–1222, <https://doi.org/10.15294/lslr.v9i1.20570>

⁷⁴ *Infopaq International A/S v Danske Dagblades Forening*, “Judgment of 16. 7. 2009 — Case c-5/08: Judgment of the Court (Fourth Chamber) 16 July 2009,” 2009.

intellectual creation, reflecting their personality and expressing free and creative choices in the photographic process. The Court emphasized that even realistic or conventional photographs may enjoy full copyright protection provided they exhibit originality in aspects such as composition, lighting, framing, and expression. Importantly, the Court rejected the notion that portrait photography receives “weaker” protection due to limited creative freedom, declaring that once originality is established, the legal protection afforded is equal to that of any other copyrighted work.⁷⁵

Applied to AI-assisted and hybrid creative workflows, *Painer* reinforces the relevance of human selection and compositional judgment as markers of originality. Where a human creator determines framing, composition, aesthetic direction, or the final selection among multiple AI-generated outputs, the resulting work may plausibly bear the imprint of the author’s personality, even if algorithmic processes are involved. However, *Painer* also underscores the limits of EU doctrine: originality remains anchored in identifiable human expression. Where AI systems operate with minimal or no human intervention, the jurisprudence provides no doctrinal mechanism to attribute personality or authorship, leaving such outputs outside the protective scope of copyright law. This tension highlights the need for clarification rather than doctrinal abandonment within the EU framework.

Furthermore, the Court clarified the scope of quotation exceptions under Article 5(3)(d) of Directive 2001/29/EC, which affirms that quotation exceptions are permitted even when the quoting work, such as a news article or press publication, is not itself protected by copyright, as long as the quoted material has been lawfully made available to the public, the quotation serves a legitimate purpose such as criticism or review, the source and author are acknowledged (unless impossible), and the use conforms to the standards of fair practice and proportionality required for the intended context.⁷⁶ The Court also held that public

⁷⁵ Eva-Maria Painer v Standard VerlagsGmbH and Others (Third Chamber), “Judgment of 1. 12. 2011 — Case C-145/10 Judgment of the Court (Third Chamber) 1 December 2011,” 2011.

⁷⁶ European Union law, “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,” 2021, see article 5(3)(d).

security exceptions under Article 5(3)(e) must be narrowly interpreted: media entities cannot invoke public security autonomously but may only do so in coordination with competent authorities, thereby preserving the balance between copyright enforcement and public interest imperatives.⁷⁷

Such case law firmly excludes purely automated or mechanical outputs from protection, underscoring the EU's continued insistence that authorship must be linked to human intellectual effort. Although more open to dynamic interpretation, the EU framework ultimately rejects the attribution of rights to AI-generated works absent substantial human intervention.

Yet these doctrinal cornerstones were forged in a pre-AI era. The rise of generative models and AI-assisted creativity has tested the elasticity of the EU's originality framework. With prompt engineering, algorithmic collaboration, and partial AI authorship now central to artistic production, the question arises whether the traditional originality test anchored in human autonomy remains viable. While the EU's Artificial Intelligence Act, which entered into force in August 2024, does not amend copyright legislation directly, it codifies a systemic boundary: the absence of substantial human involvement disqualifies AI-generated outputs from enjoying IP protection. This is evident in its consistent exclusion of copyright-related rights from the obligations imposed on general-purpose AI providers under Chapter V and Article 50 on transparency.⁷⁸

Moreover, Articles 85 and 86 entrench a rights-based framework centered on human impact and procedural clarity, but they do not grant authorial status or moral rights to AI systems. Even in the regulation of high-risk AI and synthetic content (Articles 50–52), the emphasis remains on transparency, labelling, and human oversight, rather than redefining authorship. The EU thus reaffirms its anthropocentric baseline: creativity is protectable only insofar as it is human-driven, regardless of the technical complexity or societal prominence of the AI

⁷⁷ European Union law.

⁷⁸ European Union law, "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Artificial Intelligence (Artificial Intelligence Act) (2024).," 2024.

involved. This stance preserves legal certainty within the *Acquis Communautaire*,⁷⁹ while leaving open the normative tension between innovation and tradition in intellectual property law.

Recent judicial developments in the EU have begun to recalibrate foundational copyright concepts in light of technological disruption. In *Levola Hengelo v. Smilde Foods* (Case C-310/17), the Court of Justice rejected copyright protection for the taste of a food product, holding that a “work” under Directive 2001/29/EC must be “expressed in a manner which makes it identifiable with sufficient precision and objectivity.” This articulation introduced a heightened evidentiary threshold that now resonates far beyond sensory-based claims. In disputes over AI-generated content where creative outputs often emerge from algorithmic processes without a stable or human-expressible form, the *Levola* standard casts doubt on whether such works can ever satisfy the criteria for protectable expression. While not originally intended to address machine-generated creativity, the judgment is increasingly cited as a conceptual anchor for denying protection to outputs lacking verifiable human input or expressibility.⁸⁰

This As legal scholar Vincenzo Iaia underscores in his 2024 article in *World Intellectual Property*, the European Union’s continued reliance on an anthropocentric and fragmented interpretation of originality risks entrenching systemic ambiguity at the heart of copyright law.⁸¹ Despite the growing prominence of AI-assisted creativity and transnational digital production, the EU has yet to adopt harmonized thresholds or binding standards that clearly delineate the scope of protectable subject matter when algorithmic input is involved.⁸² This regulatory inertia, Iaia argues, threatens to ossify the doctrine of originality into a fractured

⁷⁹ *Acquis communautaire* refers to the entire body of common rights and obligations that are binding on all EU Member States, including EU treaties, legislation, case law, and principles. It is the legal foundation that candidate countries must adopt before joining the European Union.

⁸⁰ *Levola Hengelo BV v. Smilde Foods BV*, “Case C-310/17,” 2018.

⁸¹ Vincenzo Iaia, “The Elephant in the Room of EU Copyright Originality: Time to Unpack and Harmonize the Essential Requirement of Copyright,” *The Journal of World Intellectual Property* 28, no. 2 (July 2025): 471–90, <https://doi.org/10.1111/jwip.12343>.

⁸² Iaia.

orthodoxy, where divergent member state practices and unpredictable judicial interpretation produce inconsistent outcomes across jurisdictions.⁸³ As a result, emerging works of algorithmic expression, particularly those generated through cross-border or multilingual generative systems, remain vulnerable to exclusion from copyright protection.⁸⁴

Such doctrinal uncertainty has broader implications. It incentivizes forum shopping, undermines the internal coherence of the Digital Single Market, and diverts creators toward private ordering solutions or jurisdictions with more predictable standards.⁸⁵ Unless the EU clarifies both the evidentiary criteria and the substantive legal threshold required for works involving AI co-authorship or automation, it risks falling behind the very technological frontier it purports to regulate.⁸⁶ In this context, Iaia's call for harmonized originality metrics and a regulatory framework that reflects the realities of human-machine collaboration is not merely doctrinal but essential for safeguarding legal certainty, creative inclusion, and market accessibility within the EU copyright regime.

Meanwhile, developments across Asia and ASEAN further illustrate the global complexity of partial AI authorship, as pragmatic experimentation and regulatory diversity shape the region's distinctive landscape of digital rights innovation. The limited translation of ASEAN-level principles into substantive intellectual property reform reflects structural socio-legal constraints rather than mere regulatory inertia. In jurisdictions such as Vietnam and Thailand, intellectual property law reform remains closely tied to economic development strategy, foreign investment stability, and administrative enforceability rather than doctrinal innovation. Courts play a relatively restrained role in developing copyright doctrine, and legislative reform tends to prioritize regulatory control, risk management, and international compliance over rights expansion. As a result, AI governance initiatives in these jurisdictions focus on transparency, labeling, and harm

⁸³ Iaia.

⁸⁴ Iaia.

⁸⁵ Iaia.

⁸⁶ Iaia.

prevention rather than rethinking authorship or originality. This institutional configuration helps explain why more experimental approaches, such as China's judicial recognition of AI-assisted authorship, have not been readily adopted within the ASEAN context.

China has positioned itself as a regulatory frontrunner in governing AI-generated content, combining flexible copyright principles with infrastructure-level legal innovations. The 2023 Guidelines on AI-Generated Content issued by the Beijing Internet Court, articulated through its decision in *Li v Liu*, affirm that AI-assisted works may receive copyright protection under Chinese law when they reflect "significant human intellectual input." Drawing from the Court's detailed reasoning, such input includes the design and sequencing of prompts, the setting of model parameters, iterative refinement, and aesthetic judgment applied during the generation process. The Court emphasized that these acts constitute personalized expression and intellectual achievement under China's Copyright Law, thereby distinguishing the resulting work from mere mechanical output. This position establishes a practical threshold of human involvement that contrasts sharply with the more rigid human-authorship requirement seen in jurisdictions like the United States, while offering a doctrinal path to copyright recognition for hybrid human–AI creations.⁸⁷ This interpretation aligns with China's emerging legislative framework under the Artificial Intelligence Law of the People's Republic of China (Draft for Suggestions from Scholars). Articles 85 to 90 of the Draft Law articulate differentiated liability regimes based on the degree of control and foreseeability of harm. Article 85 introduces general fault-based liability for AI users or developers who cause harm through negligent use. Article 86 establishes strict liability for high-risk AI systems that operate with a high degree of autonomy and pose foreseeable danger. Article 87 provides a safe harbor clause for service providers, contingent upon timely removal of infringing content upon notification. Article 90 imposes direct civil and administrative liability on foundational model

⁸⁷ Stanley Lai et al., "Legal Implications – Beijing Internet Court Grants Copyright Protection to AI-Generated Artwork," 2024.

developers if their outputs violate third-party rights, mislead users, or circumvent regulatory safeguards.⁸⁸

Concurrently, China has embedded evidentiary modernization into its legal infrastructure. Complementing this framework, Articles 62 and 64 of the Draft AI Law empower regulatory authorities to establish comprehensive risk identification and classification mechanisms for critical AI systems. These provisions mandate that developers and deployers of high-risk AI tools implement technical safeguards, audit trails, and data provenance systems to ensure accountability throughout the AI lifecycle. The law further allows authorities to require third-party evaluations, usage monitoring, and real-time flagging of harmful outputs.⁸⁹ By embedding these operational duties into enforceable legal norms, the Chinese model advances a proactive, infrastructure-level regulatory architecture that anticipates misuse and system failures before they result in harm.

This regulatory framework has moved beyond normative aspiration into judicial enforcement. In April 2025, the Beijing Tongzhou District People's Court issued China's first criminal conviction involving the misuse of AI in copyright infringement. Four individuals were found guilty of downloading artistic works from online platforms, processing them via open-source AI models into derivative puzzles, and commercializing them without permission. The court imposed custodial sentences ranging from imprisonment to probation, along with individual fines up to 60,000 yuan. Additionally, the Fuzhou-based e-commerce company facilitating the sales was fined 100,000 yuan and held jointly liable as a legal person, establishing a precedent for unit crime under the corporate liability doctrine. Notably, the court emphasized the defendants' failure to implement adequate content filtering, user risk warnings, and provenance checks as aggravating factors. The prosecutorial office further highlighted the evidentiary importance of communication logs, algorithmic tracing, and visual similarity analysis, especially where AI use obfuscates direct copying.

⁸⁸ Zhang Linghan et al., "Artificial Intelligence Law of the People's Republic of China (Draft for Suggestions from Scholars)," *Center for Security and Emerging Technology*. Accessed: Aug 16 (2024).

⁸⁹ Linghan et al.

This case not only affirms the applicability of China's Criminal Law to AI-related infringements but also demonstrates judicial willingness to adapt enforcement tools to emerging technological misuse.⁹⁰ New forms of technology have made the death penalty more salient in a range of criminal execution laws.⁹¹

Japan has recently transitioned from a soft-law, principle-based approach to a formal legislative framework in regulating artificial intelligence. This shift is marked by the enactment of the Act on Promotion of Research and Development and Utilization of Artificial Intelligence-Related Technologies ("AI Bill") on 28 May 2025, which constitutes Japan's first dedicated statute on AI governance. Rather than imposing binding prohibitions, the AI Bill takes an innovation-first, cooperation-based approach. It outlines national strategies to promote R&D and ensure responsible AI utilization, emphasizing transparency, international collaboration, and the protection of human rights. The Act designates the Prime Minister as the chair of the AI Strategic Headquarters, with all Cabinet ministers as members, tasked with formulating AI policy and coordinating with administrative agencies. Basic measures include promoting AI research, expanding data infrastructure, ensuring human resources and education, establishing international guidelines, and collecting information on rights infringements. Business operators are expected to cooperate with government initiatives, while the government is responsible for reviewing and updating measures as needed. Overall, the act aspires to make Japan a global model for AI regulation, balancing economic growth, security, and ethical safeguards.⁹²

Although the AI Bill does not stipulate fines or penalties, the combination of investigatory powers and naming-and-shaming mechanisms provides implicit enforcement pressure. To supplement this

⁹⁰ Fei Dang, "Beijing Court Sentences Four People for Infringing Copyright by Using AI," 2025.

⁹¹ Anis Widyawati et al., "Dynamics of the Penitentiary System, Transparent, and Accountable Handling of Criminal Cases in Criminal Execution Law in Southeast Asia: Convergence and Divergence of International Perspectives," *Indonesia Law Review* 15, no. 1 (2025): 18, <https://doi.org/10.15742/ilrev.v15n1.1>.

⁹² Japanese Law Translation, "Outline of the Act on Promotion of Research and Development, and Utilization of AI-Related Technology (AI Act)," 2025.

statutory framework, the government has issued the AI Guidelines for Business (v1.0 in 2023, updated through March 2025), which articulate operational expectations in areas such as human rights, privacy, fairness, cybersecurity, accountability, and education.⁹³ These guidelines, though non-binding, serve as interpretive tools for compliance and are widely observed across industries. The AI Guidelines v1.0 Part 2C, in particular, emphasize traceability, explainability, and internal capacity-building to align AI usage with public trust and risk-based principles.⁹⁴

Further direction is provided by the Interim Report of the AI Regulation Research Group (Feb 2025), which affirms Japan's commitment to a post-market regulatory model prioritizing transparency obligations and cooperative auditing over rigid ex-ante restrictions.⁹⁵ This model is externally projected through Japan's leadership in formulating the Hiroshima International Guiding Principles for Advanced AI Systems, which delineate normative standards to mitigate risks including disinformation, IP abuse, health and safety threats, and systemic algorithmic discrimination.⁹⁶

In parallel, Japan's General Understanding on AI and Copyright (March 2024) clarifies that training AI models on copyrighted content is generally permissible under Japan's copyright exceptions, provided that such use does not cause unreasonable harm to rights holders. However, copyright protection for AI-generated outputs is not automatically granted; it requires demonstrable human intellectual contribution, in line with the traditional requirement of authorship under the Copyright Act.⁹⁷

Despite this formal flexibility, Japan has not translated permissive data mining exceptions into a more expansive doctrine of authorship.

⁹³ Ministry of Internal Affairs and Communications, "Japan Conference Toward AI Network Society, AI Guidelines for Business – Version 1.0," 2021.

⁹⁴ Ministry of Internal Affairs and Communications, "Japan Conference Toward AI Network Society, Interim Report on the Vision for Future Society Transformed by AI," 2019.

⁹⁵ David Albagli et al., "AI Watch: Global Regulatory Tracker - Japan," 2025.

⁹⁶ Ministry of Foreign Affairs of Japan, "Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems," 2024.

⁹⁷ Japan Copyright Office, "General Understanding on AI and Copyright in Japan," 2024.

One explanation lies in the continued doctrinal centrality of human authorship within Japanese copyright law, which remains closely tied to personal expression and moral rights. While the legal system tolerates broad computational use of copyrighted materials at the input stage, it remains institutionally resistant to recognizing AI-mediated outputs as protectable works absent clearly identifiable human creative intent. This separation between data permissibility and authorship attribution reflects a cautious, incrementalist approach: Japan prioritizes legal certainty and industrial coordination over doctrinal experimentation, leaving any recalibration of authorship to explicit legislative action rather than judicial interpretation.

In addition to legislative and policy developments, recent jurisprudence in Japan reaffirms the country's strict adherence to anthropocentric standards of inventorship and authorship in the context of artificial intelligence. In 2024, the Intellectual Property High Court upheld the Tokyo District Court's decision to reject a legal challenge brought by a U.S. engineer seeking to overturn the Japan Patent Office's refusal to recognize an AI system, DABUS (Device for the Autonomous Bootstrapping of Unified Sentience), as the inventor in a patent application. Presiding Judge Hibiki Shimizu emphasized that, under Japanese patent law, the status of "inventor" is limited to natural persons. The Court held that granting inventorship status to AI would exceed the scope of interpretation of the existing statutory framework, noting that such systemic changes should be approached through legislative deliberation aligned with national industrial policy. The ruling affirms Japan's doctrinal position that AI-generated inventions or creative outputs fall outside the current legal entitlement to patent protection unless human creative input can be distinctly identified and attributed.⁹⁸

Together, these instruments reflect Japan's evolving regulatory architecture, combining soft guidance, investigatory authority, and principle-based duties to promote innovation while addressing the legal uncertainties and societal risks posed by advanced AI systems.

Contrary to the legislative codification observed, Singapore has, as of July 2025, deliberately refrained from enacting a dedicated,

⁹⁸ Excel V. Dyquiango, "Japan High Court Upholds Rejection of AI as Inventor in Patent Case," *Asia IP*, 2025.

overarching law on artificial intelligence. Instead, Singapore adopts a pragmatic, risk-based governance model characterized by international interoperability, regulatory experimentation, and sector-specific adaptability. Under this approach, legal interventions are tailored to discrete AI use cases, with risks typically addressed under existing statutory frameworks—most notably the Personal Data Protection Act, intellectual property law, and consumer protection statutes.⁹⁹

This regulatory ethos is anchored in Singapore’s National AI Strategy (NAIS), initially launched in 2019 and extensively revised with the release of NAIS 2.0 in December 2023. The updated strategy articulates Singapore’s aspiration to position itself as a global hub for “AI innovation and deployment in the public interest,” with an explicit focus on social trust, economic competitiveness, and digital resilience.¹⁰⁰ NAIS 2.0 envisions Singapore as a “Living Lab for AI,” actively supporting real-world piloting of AI solutions, cross-sectoral risk management, and the operationalization of responsible governance practices.¹⁰¹

To realize this vision, Singapore has introduced a suite of soft-law instruments and operational guidelines. The Model Artificial Intelligence Governance Framework (2019, revised 2020) from the Infocom Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC) sets out voluntary, cross-sector principles emphasizing transparency, explainability, fairness, and human-centricity.¹⁰² In May 2024, this framework was supplemented by the Model AI Governance Framework for Generative AI, which articulates nine key governance dimensions for GenAI, including accountability across the AI value chain, robust model evaluation, content provenance, and mandatory incident reporting.¹⁰³

⁹⁹ Lim Chong Kin and Cheryl Seah, “Artificial Intelligence 2025 - Singapore | Global Practice Guides | Chambers and Partners,” 2025.

¹⁰⁰ Smart Nation and Digital Government Office, *Singapore National AI Strategy 2.0*, 2023.

¹⁰¹ Smart Nation and Digital Government Office.

¹⁰² Infocomm Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC), “Model Artificial Intelligence Governance Framework (Second Edition),” 2020.

¹⁰³ AI Verify Foundation Infocomm Media Development Authority (IMDA), “Model AI Governance Framework for Generative AI,” 2024.

On the technical assurance front, Singapore has established AI Verify (launched 2022) as a national framework for testing AI systems against 11 internationally accepted principles, combining both technical and process-based audits. This was expanded with the rollout of Project Moonshot in 2024, which provides curated benchmarks and red-teaming protocols for evaluating large language models (LLMs).¹⁰⁴ Importantly, the AI Verify framework has been mapped to both the U.S. National Institute of Standards and Technology (NIST) AI Risk Management Framework and the ISO/IEC 42001:2023 international standard, underscoring Singapore's commitment to global harmonization in AI governance.¹⁰⁵

Sectoral guidelines further complement this architecture. Notably, the Monetary Authority of Singapore (MAS) has issued the Principles to Promote Fairness, Ethics, Accountability, and Transparency (FEAT) for the financial sector, while the Ministry of Health (MOH), Health Sciences Authority (HSA), and Integrated Health Information Systems have jointly developed the Artificial Intelligence in Healthcare Guidelines to steer responsible AI adoption in healthcare.¹⁰⁶ For emerging applications such as autonomous vehicles, Singapore regulates AI-enabled systems under general laws like the Road Traffic Act and the Health Products Act, thereby demonstrating a pragmatic preference for adapting existing statutory regimes over premature, sector-wide codification.¹⁰⁷

Ultimately, Singapore's regulatory strength lies in its agility and iterative policy design. Rather than imposing rigid legislative requirements that may struggle to keep pace with technological innovation, agencies such as IMDA and PDPC continually refine their

¹⁰⁴ Infocomm Media Development Authority (IMDA), "Singapore Launches Project Moonshot," IMDA, 2024.

¹⁰⁵ AI Verify Foundation, "What Is AI Verify – AI Verify Foundation," 2025.

¹⁰⁶ Monetary Authority of Singapore, "Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector," 2019; Health Sciences Authority (HSA), "Integrated Health Information Systems (IHIS) Ministry of Health (MOH), Artificial Intelligence in Healthcare Guidelines (AIHGle)," 2021.

¹⁰⁷ Road Traffic Act 1961, "Singapore Statutes Online," 2020; Health Products Act, "Singapore Statutes Online 2007," 2020.

methodologies for AI testing and assurance, engaging industry stakeholders through public consultation and cross-border standard alignment. This approach allows Singapore to maintain a dynamic balance between regulatory certainty, practical enforceability, and ongoing support for innovation, positioning the nation as a global reference for principled, adaptive AI governance.

By contrast with Singapore's sectoral and adaptive strategy, Vietnam enacted the Digital Technology Industry Law (DTI Law) in June 2025, which will be effective from January 2026 and establishes the country's first comprehensive legal framework for digital technology and artificial intelligence. The DTI Law applies to both domestic and foreign entities involved in digital technology activities, encompassing hardware and software production, digital content, and a broad range of services, including consulting, integration, and data processing. Most notably, the DTI Law introduces a formal definition of AI systems consistent with OECD principles and mandates a human-centric, risk-based approach to AI governance. Key requirements include transparency, labelling of AI-generated products, ongoing risk management, and human oversight throughout the AI lifecycle. The law classifies AI applications by risk level, with high-risk systems subject to enhanced regulatory scrutiny, and entrusts the Ministry of Science and Technology with issuing further implementation standards. Additionally, the DTI Law establishes the first clear legal framework for digital assets, prohibits unjustified data localization barriers and technical measures that restrict data portability, and provides for regulatory sandboxes, investment incentives, and talent development, underlining Vietnam's ambition to accelerate digital transformation while ensuring regulatory certainty and alignment with international norms.¹⁰⁸

Transitioning from the regulatory experimentation seen in Singapore and the risk-based statutory regime adopted by Vietnam, Thailand has embarked on a national strategy that places significant emphasis on both regulatory preparedness and ecosystem development for artificial intelligence. The Thailand National AI Strategy and Action Plan (2022–2027), which received final cabinet approval in July 2022,

¹⁰⁸ Sudhanshu Singh, "Vietnam Passes First-Ever Law on Digital Technology Industry," 2025.

serves as the foundational policy roadmap for the country's AI governance and future regulation.¹⁰⁹

Thailand's approach is notable for its explicit acknowledgment of the gaps in AI-specific laws, ethics, and regulatory frameworks.¹¹⁰ The strategy outlines five integrated pillars: (1) preparing readiness in social, ethics, law, and regulation; (2) developing infrastructure for sustainable AI; (3) increasing human capability and AI education; (4) driving technology and innovation development; and (5) promoting the use of AI in both public and private sectors.¹¹¹ A central commitment of the NAIS is to have an enforceable AI law and regulatory standards in place by 2027, supported by wide-reaching awareness and education programs on AI ethics, with a stated goal of reaching at least 600,000 Thais.¹¹²

The plan adopts a holistic governance vision: regulatory and policy initiatives are to be overseen by the National AI Committee, chaired by the Prime Minister, and supported by sectoral regulators, research institutes, and dedicated subcommittees.¹¹³ This centralization ensures both policy coherence and multi-sectoral engagement, ranging from digital business and telecoms to academia and public sector stakeholders.

In terms of substantive regulatory direction, Thailand's NAIS integrates global best practices, notably promoting a risk-based, human-centered, and accountable AI ecosystem. It calls for clear policies and standards for AI ethics, legal mandates for risk management and human oversight, and mechanisms for public notification and redress in high-risk AI use cases.¹¹⁴ Regulatory sandboxes are envisaged as key

¹⁰⁹ National Science and Technology Development Agency (NSTDA) and Office of the National Digital Economy and Society Commission (ONDE), "Thailand National AI Strategy and Action Plan (2022–2027)," 2022.

¹¹⁰ National Science and Technology Development Agency (NSTDA) and Office of the National Digital Economy and Society Commission (ONDE).

¹¹¹ National Science and Technology Development Agency (NSTDA) and Office of the National Digital Economy and Society Commission (ONDE).

¹¹² National Science and Technology Development Agency (NSTDA) and Office of the National Digital Economy and Society Commission (ONDE).

¹¹³ National Science and Technology Development Agency (NSTDA) and Office of the National Digital Economy and Society Commission (ONDE).

¹¹⁴ National Science and Technology Development Agency (NSTDA) and Office of the National Digital Economy and Society Commission (ONDE).

mechanisms for supporting business innovation and AI startups, echoing trends in the region.¹¹⁵

The strategy further prioritizes the creation of robust national infrastructure, including AI expert networks, data analytics platforms, and high-performance computing resources, and commits to producing over 30,000 AI professionals within six years.¹¹⁶ Ambitious economic targets are set, aiming for more than 100 R&D prototypes, the integration of AI across at least 600 public and private agencies,¹¹⁷ and measurable impacts on productivity, digital transformation, and social welfare.

A review of the legal treatment of partial and AI-generated authorship across Asia reveals marked differences in both statutory approach and practical enforceability. In China, authorship of AI-generated works is not recognized under copyright law, but providers are strictly required to label and control the distribution of AI-generated content, reflecting a regulatory priority on governance over ownership. Japan, despite early adoption of AI principles, still leaves the legal status of AI-generated authorship unresolved, with no explicit statutory protection and ongoing reliance on traditional copyright thresholds. Singapore's legal environment promotes transparency and accountability through assurance frameworks and sectoral codes, yet does not extend copyright to non-human creators, maintaining a clear distinction between human and machine authorship. Vietnam's new digital technology law introduces transparency, labeling, and risk management obligations for AI systems but stops short of granting legal authorship to AI, instead focusing on compliance and human oversight. In Thailand, while policy targets emphasize enforceable AI law and ethics, current intellectual property law continues to limit copyright protection to works created by natural persons, leaving hybrid and AI-generated art in a legal grey zone.

¹¹⁵ National Science and Technology Development Agency (NSTDA) and Office of the National Digital Economy and Society Commission (ONDE).

¹¹⁶ National Science and Technology Development Agency (NSTDA) and Office of the National Digital Economy and Society Commission (ONDE).

¹¹⁷ National Science and Technology Development Agency (NSTDA) and Office of the National Digital Economy and Society Commission (ONDE).

Collectively, these jurisdictions illustrate that, despite growing policy attention to transparency and human oversight, statutory authorship and copyright for AI-generated or hybrid works remain largely unrecognized across Asia. Most national regimes continue to subordinate questions of ownership to broader concerns about risk, accountability, and market development. This persistent legal gap not only hinders the enforceability of rights in AI-assisted creativity but also highlights the need for regional coordination, setting the stage for ASEAN's recent push to encourage member states to adopt common frameworks for AI regulation and governance.

As the OECD notes while many countries have advanced AI policy initiatives, differences in national regulatory frameworks and technical capacity continue to complicate international harmonisation and interoperability.¹¹⁸

In response to these challenges, ASEAN's approach to AI regulation is shaped by its ambition to become a leading digital community and economic bloc, supported by secure and transformative digital services, technologies, and an integrated ecosystem. As outlined in the ASEAN Digital Masterplan 2025, member states have acknowledged the need to develop and adopt a regional policy framework to guide best practices in AI governance and ethics. While recent years have seen a proliferation of national and international principles and frameworks, such as Singapore's Model AI Governance Framework and the OECD Recommendation on AI, ASEAN has not yet established a formal intergovernmental common standard for AI. Instead, current regional efforts focus on providing guidance for policymakers and organizations to design and utilize AI systems in a responsible and ethical manner, with reference to global guidelines such as UNESCO's Recommendation on the Ethics of Artificial Intelligence and the EU's Guidelines for Trustworthy AI. The ASEAN Guide on AI Governance and Ethics itself aims to support these efforts by offering regional principles to increase users' trust and promote responsible AI development and deployment across Southeast Asia.¹¹⁹

¹¹⁸ OECD/KDI, *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses*.

¹¹⁹ ASEAN, "ASEAN Guide on AI Governance and Ethics Contents," 2024.

The intersection of artificial intelligence and copyright law now exposes the limits of established legal doctrine, as machine-augmented creativity renders traditional concepts of authorship, originality, and ownership increasingly unstable. The blurred lines between permissible and impermissible transformative use are especially salient as courts, regulators, and platforms attempt to reconcile the creative potential of AI systems with longstanding copyright doctrines. The legal outcomes depend not only on the technical processes by which AI systems acquire, process, and reuse data, but also on how decision-makers interpret the transformative character and economic impact of each use in light of evolving market realities. Across Asia, as elsewhere, the legal treatment of partial and AI-generated authorship remains mired in doctrinal inertia and fragmented statutory frameworks. Leading jurisdictions—including China, Japan, Singapore, Vietnam, and Thailand have yet to articulate enforceable pathways for recognizing or protecting hybrid or machine-generated works, leaving creators and rights holders in a persistent legal grey zone. This patchwork approach not only undermines legal certainty and innovation incentives but also heightens the risk of regulatory arbitrage and cross-border disputes. Absent regional or international harmonization, the governance of AI-generated creativity will remain contested and provisional, defined as much by ongoing negotiation between technical, economic, and normative interests as by settled law.

B. Empirical Realities: The Market Effects of Legal Uncertainty

The doctrinal ambiguity explored in the previous section is not merely theoretical; it produces immediate and far-reaching economic consequences for digital creative markets. As AI-generated and hybrid works become mainstream, platforms that facilitate digital ownership, such as NFT marketplaces, have emerged as critical sites of legal and economic experimentation. In these spaces, the absence of clear rules around originality, attribution, and rights allocation has become a central source of volatility, commercial risk, and systemic exclusion. For creators and investors alike, empirical studies reveal that the uncertainty of enforceable rights, especially in cases involving partial AI authorship,

now constitutes a major barrier to market participation and investment.¹²⁰

The recent evolution of NFT platforms highlights this complexity: as partial AI-generated art is increasingly minted and traded, the market has witnessed dramatic swings in value and changing patterns of participation. In 2023, the oft-cited claim that “95% of NFTs are now worthless,” based on market data reviewed by WAC Lab, reflected the dramatic decline in value for the majority of NFT projects, especially in collectibles, though the picture is more nuanced for digital and generative art sectors.¹²¹ For hybrid and AI-generated art, while market downturns have reduced liquidity and price stability, the diversity of use cases and ongoing creative activity mean that these categories may be more resilient than pure collectibles. Nevertheless, persistent questions about originality and rights enforcement in mixed-authorship works continue to challenge both market and legal confidence in the sector.¹²²

The fragmented legal frameworks across major jurisdictions further intensify this instability. In the United States, copyright protection is, by statute and long-standing policy, strictly limited to works created by human authors: Sections 802.5(C) and 808.7(C) of the U.S. Copyright Office Compendium provide, “The Office will refuse to register a claim if it determines that a human being did not create the work” (U.S. Copyright Office Compendium, §§ 802.5(C), 808.7(C)).¹²³ This position has been reaffirmed in recent case law, notably *Thaler v. Perlmutter* (D.D.C. 2023).¹²⁴ Similarly, in the European Union, both the InfoSoc Directive (Directive 2001/29/EC) and the Court of Justice of

¹²⁰ Andrei Hagiu and Julian Wright, “Artificial Intelligence and Competition Policy,” *International Journal of Industrial Organization*, 2025, 12–14, <https://doi.org/10.1016/j.ijindorg.2025.103134>; NFTGO, “NFT Annual Report 2024,” 2024, Chapter 1, 8; Chapter 2, pp. 17, Chapter 4, page 52.

¹²¹ WAC Lab, “Are 95% Of NFTs Really Worthless? Let’s Take A Closer Look At The Market,” Web3 for the Arts and Culture, 2023.

¹²² Ali Masyhar et al., “Legal Challenges of Combating International Cyberterrorism: The NCB Interpol Indonesia and Global Cooperation,” *Legality: Jurnal Ilmiah Hukum* 31, no. 2 (2023), <https://doi.org/10.22219/ljih.v31i2.29668>.

¹²³ U.S. Copyright Office, “Compendium of U.S. Copyright Office Practices, Third Edition, §§ 802.5(C), 808.7(C)” (2021).

¹²⁴ *Perlmutter*, “United States District Court for the District of Columbia: Memorandum Opinion.”

the European Union (CJEU) have consistently defined the “author” as a natural person, confirming that copyright subsists only in works reflecting the author’s own intellectual creation (CJEU, *Infopaq C-5/08*; *Painer C-145/10*).¹²⁵ By contrast, several Asian jurisdictions, notably China and Japan, have adopted a more flexible approach. In China, the Beijing Internet Court has recognized that copyright may subsist in AI-assisted works if “significant human intellectual input” can be demonstrated, such as through prompt engineering or iterative human editing (Beijing Internet Court, *Li v. Liu*, 2023; PRC Copyright Law).¹²⁶ Japan’s recent General Understanding on AI and Copyright (2024) and its updated guidelines also permit copyright protection for AI-generated outputs where substantial human contribution is evident, though the baseline requirement of human authorship remains.¹²⁷

This patchwork of jurisdiction-specific approaches produces not only doctrinal uncertainty but also profound market instability for artists and creators operating in the global NFT and AI art economy. As AI-generated NFTs proliferate, the absence of harmonized legal standards around authorship, originality, and intellectual property has created persistent ambiguities for both creators and collectors. In practice, as highlighted by *Blockchain Today*, this evolving legal landscape encourages what legal scholars describe as “regulatory arbitrage” and “forum shopping,” as artists and platforms seek out jurisdictions or NFT marketplaces with the most favorable or least restrictive rules—a dynamic clearly reflected in the shifting policies and business strategies noted across leading NFT platforms. Such strategic maneuvering often benefits technologically sophisticated or well-resourced actors, while less-resourced creators—particularly those from emerging markets—face greater barriers to entry, fewer opportunities for effective remedy, and increased risk of exclusion from the economic value generated by this new creative economy. While the innovative potential of AI-generated NFTs has democratized access and expanded creative possibilities, it has also heightened the urgency for greater transparency, balanced

¹²⁵ *Infopaq International A/S v Danske Dagblades Forening*, “Judgment of 16. 7. 2009 — Case C-5/08: Judgment of the Court (Fourth Chamber) 16 July 2009.”

¹²⁶ *AWAPoint*, “China’s First AI-Generated Picture Copyright Infringement Case: Legal Implications.”

¹²⁷ Japan Copyright Office, “General Understanding on AI and Copyright in Japan.”

regulation, and inclusive governance to ensure that the benefits of this emerging digital art ecosystem are more equitably shared.¹²⁸

In sum, the evolving legal and technical landscape of partial AI authorship and digital asset platforms highlights a fundamental paradox: while legal uncertainty and fragmented governance can foster innovation and experimentation, they just as often deepen instability, exclusion, and the concentration of value and power. The empirical record underscores that without harmonized, inclusive legal frameworks and greater support for less-resourced and marginalized creators, advances in digital technology risk perpetuating old inequities under new guises. This dynamic, sometimes described as an ‘innovation paradox’ or ‘paradox of openness,’ aligns with what open innovation theory and Coasean economics predict: in environments characterized by high uncertainty and increased transaction costs, the benefits of innovation and knowledge sharing tend to be captured primarily by dominant, well-resourced actors, while less powerful participants remain exposed to the risks of value appropriation and systemic exclusion.¹²⁹

C. Blockchain Evidence and Legal Certainty: Provenance, Attribution, and Trust Across Jurisdictions

The allure of blockchain technology, often described as a distributed ledger of records which are absolute and certifiable, lies in its ability to provide immutable, time-stamped records that are transparent and resistant to tampering.¹³⁰ In digital art and NFT markets, the core characteristic of blockchain technology, namely its ability to create immutable, time-stamped, and tamper-resistant records, enables not only robust attribution of authorship but also the potential for automated rights transfers, effectively eliminating the need for trusted third parties

¹²⁸ Blockchain Today, “AI-Generated NFTs and Their Impact on the Digital Art Market,” Medium, 2025.

¹²⁹ Yao Sun, Ann Majchrzak, and Arvind Malhotra, “593Open Innovation Theories,” ed. Henry Chesbrough et al., *The Oxford Handbook of Open Innovation* (Oxford University Press, February 2024), <https://doi.org/10.1093/oxfordhb/9780192899798.013.35>.

¹³⁰ Stephanie Susnjara and Ian Smalley, “What Is Blockchain?,” 2025.

in the authentication and recording of transactions. Every transaction is validated through consensus among network participants, and once entered, it cannot be erased, thus ensuring both traceability and data integrity.¹³¹

The practical impact of these features has already been recognized in the legal field, where blockchain is employed by law firms and notary services for document certification, proof of ownership, authorship attribution, and the establishment of proof of existence at a certain point in time.¹³² For instance, law firms use platforms like Stampery for document authentication, while notary functions are performed via services such as Block Notary, which utilizes TestNet3 or the Bitcoin Network, and Crypto Public Notary, both enabling documents to be recorded on the blockchain with SHA256 cryptographic hashes and minimal bitcoin payments. This legal uptake demonstrates blockchain's capacity to serve as a universal "proof of provenance," accessible and verifiable across jurisdictions.¹³³

Nevertheless, as highlighted in the technical literature, while blockchain can unequivocally demonstrate that a record existed at a specific moment, it cannot by itself guarantee the truthfulness of the underlying claim, authenticate the identity of the party asserting rights, or determine the legal validity of a transaction.¹³⁴ Thus, the certainty promised by distributed ledgers remains subject to real-world limitations, particularly regarding legal enforceability and evidentiary standards that extend beyond mere record existence.

As highlighted in the 2022 WIPO Blockchain Evidence Report, the legal status of blockchain entries in court remains unsettled across jurisdictions. While blockchain technology provides time-stamped, immutable records that can serve as powerful evidence of a work's

¹³¹ Leonardo J Ramirez Lopez and Genesis G Morillo Ledezma, "Employing Blockchain, NFTs, and Digital Certificates for Unparalleled Authenticity and Data Protection in Source Code: A Systematic Review," *Computers*, 2025, <https://doi.org/10.3390/computers14040131>.

¹³² Gurinder Singh, Vikas Garg, and Pooja Tiwari, *Introduction to Blockchain Technology, Transforming Cybersecurity Solutions Using Blockchain* (Springer, 2021), 11, https://doi.org/10.1007/978-981-33-6858-3_1.

¹³³ Singh, Garg, and Tiwari, *Introduction to Blockchain Technology*.

¹³⁴ Singh, Garg, and Tiwari.

existence or transaction at a specific moment, these records are not automatically accepted as self-authenticating proof. Instead, courts and regulators must determine, often on a case-by-case basis, whether to treat blockchain evidence as conclusive or to weigh it alongside other elements in the broader evidentiary landscape. This persistent legal ambiguity reflects broader challenges in integrating emerging technologies with traditional evidentiary standards and underscores the need for clearer procedural guidance to ensure consistent and reliable use of blockchain-based records in intellectual property and digital rights disputes.¹³⁵

A close analysis of blockchain regulation in the United States reveals not only a fragmented but also a highly dynamic legal landscape, in which the lack of federal coordination has fostered intense state-level experimentation and regulatory competition.¹³⁶ States such as Vermont have positioned themselves as legal pioneers: Vermont Statutes Annotated, Title 12, § 1913 grants blockchain-based records a presumption of authenticity as “mathematically secured, chronological, and decentralized consensus ledgers” admissible as business records.¹³⁷ Arizona amended its Uniform Electronic Transactions Act to expressly recognize blockchain-based records and signatures as legally enforceable under Ariz. Rev. Stat. § 44-7061, guaranteeing that “smart contracts may exist in commerce” and cannot be denied legal effect solely for their digital form.¹³⁸ Delaware authorized the maintenance of corporate stock ledgers and other business records on blockchain technology with Del. Code Ann. tit. 8, § 224, fundamentally integrating blockchain into its corporate law framework.¹³⁹

These states are not the only ones embracing this trend. Illinois’ Blockchain Technology Act (205 ILCS 730/1 et seq.) broadly recognizes the validity of blockchain records, smart contracts, and digital signatures in commercial transactions, while also prohibiting local governments

¹³⁵ WPO, *Blockchain Technologies and IP Ecosystems: A WIPO White Paper* (Geneva, Switzerland: World Intellectual Property Organization, 2022).

¹³⁶ Joseph Jasperse, “50-State Review of Cryptocurrency and Blockchain Regulation,” 2023.

¹³⁷ Vermont Statutes Annotated, Title 12, § 1913

¹³⁸ Ariz. Rev. Stat. § 44-7061

¹³⁹ Del. Code Ann. Tit. 8, § 224.

from restricting their use.¹⁴⁰ Nevada enacted SB 398 (2017), which not only prohibits local governments from imposing taxes or restrictions on blockchain technology but also explicitly recognizes blockchain-based records and smart contracts as electronic records under the Uniform Electronic Transactions Act (NRS 719.245).¹⁴¹ Wyoming, often regarded as the most blockchain-friendly jurisdiction, has enacted a suite of statutes, including the Wyoming Utility Token Act (Wyo. Stat. Ann. § 34-29-101 et seq.), the Special Purpose Depository Institutions Act (Wyo. Stat. Ann. § 13-12-101 et seq.), and amendments to its corporate law (HB 101, HB 185, SF 68) enabling the formation of DAOs as legal entities and the issuance of “certificate tokens” in lieu of traditional stock certificates.¹⁴²

Meanwhile, Tennessee (Tenn. Code Ann. § 47-10-201), Ohio (Ohio Rev. Code § 1306.01), Arkansas (Ark. Code Ann. § 25-32-122), South Dakota (SD Codified Laws § 53-12-1), Utah (Utah Blockchain Technology Act, 2019; Utah Code Ann. § 67-4a-102), North Dakota (HB 1045), Texas (SB 1859, HB 4214), and Washington (SB 5638, 2019) have also passed statutes affirming the legal status of blockchain records, signatures, and smart contracts, often extending legal effect to records “secured through distributed ledger technology” in commercial and governmental contexts.¹⁴³

Despite this statutory innovation, the resulting landscape is one of “islands” of legal certainty surrounded by vast uncertainty and compliance complexity. The scope of legal recognition varies widely not only in the language of each statute but also in the breadth of application: some states limit blockchain’s legal force to recordkeeping or notarial acts, while others extend it to smart contracts, digital asset property, and corporate governance.¹⁴⁴ Even within “progressive” states, the intersection of blockchain with licensing, property law, and securities

¹⁴⁰ 205 ILCS 730/1 et Seq.

¹⁴¹ NRS 719.245.

¹⁴² Wyo. Stat. Ann. § 34-29-101 et Seq.; Wyo. Stat. Ann. § 13-12-101 et Seq.

¹⁴³ Tenn. Code Ann. § 47-10-201.; Ohio Rev. Code § 1306.01.; Ark. Code Ann. § 25-32-122.; SD Codified Laws § 53-12-1.; Utah Blockchain Technology Act, 2019.; Utah Code Ann. § 67-4a-102.; HB 1045 (ND).; HB 4214 (TX).; SB 1859 (TX).; SB 5638 (WA).

¹⁴⁴ Jasperse, “50-State Review of Cryptocurrency and Blockchain Regulation.”

regulation often remains unresolved or subject to administrative interpretation, increasing regulatory risk for multi-state operators.

At the federal level, no statute directly addresses the evidentiary status or legal recognition of blockchain-based records or smart contracts. Federal courts rely primarily on Federal Rule of Evidence 901, which obliges proponents to produce evidence sufficient to support a finding that a blockchain record “is what the proponent claims it is,” commonly through expert testimony detailing the technical process, chain of custody, and the operation of the blockchain system itself.¹⁴⁵ This framework, originally developed for physical and traditional electronic documents, offers judges broad discretion and leads to varied judicial outcomes, particularly when courts must assess the authenticity of complex digital records like blockchain data without the benefit of established standards or statutory presumptions of reliability.¹⁴⁶

Federal agencies such as the SEC, CFTC, IRS, and FinCEN have approached blockchain through legacy statutory frameworks: for example, the IRS treats cryptocurrencies as property for tax purposes under IRS Notice 2014-21; FinCEN classifies many digital asset businesses as Money Services Businesses under the Bank Secrecy Act (31 U.S.C. § 5311 et seq.); and the CFTC and SEC have asserted jurisdiction over digital asset markets primarily through enforcement actions rather than proactive rulemaking.¹⁴⁷ None have issued regulations directly addressing the evidentiary admissibility or legal reliability of blockchain records.

The cumulative effect is a regulatory environment in which legal certainty and enforceability of blockchain records, smart contracts, and digital asset transactions remain contingent upon the particular statutory

¹⁴⁵ Federal Rules of Evidence, “Rule 901: Authenticating or Identifying Evidence,” 2025.

¹⁴⁶ Federal Rules of Evidence.

¹⁴⁷ Internal Revenue Service, *IRS Notice 2014-21: Guidance on Virtual Currency*, 2014; Bank Secrecy Act, 31 U.S.C. § 5311 et Seq; Financial Crimes Enforcement Network (FinCEN), “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies (FIN-2019-G001),” 2019; U.S. Commodity Futures Trading Commission, “CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets,” 2018; U.S. Securities and Exchange Commission, “Framework for ‘Investment Contract’ Analysis of Digital Assets,” 2019.

regime and forum. For practitioners, this means navigating a complex web of state statutes and administrative interpretations ranging from Vermont Stat. Ann. tit. 12, § 1913 to the Wyoming Utility Token Act and Nevada SB 398 with no unifying federal standard. Until a harmonized national framework or binding judicial precedent emerges, the US will remain a jurisdiction where statutory innovation, legal uncertainty, and regulatory arbitrage coexist, shaping both the risks and opportunities for blockchain-based business models.¹⁴⁸

In *United States v. Sterlingov*, one of the most high-profile prosecutions involving blockchain forensics, the court admitted extensive blockchain-based records, including evidence of cryptocurrency transactions and wallet associations derived from analysis of the Bitcoin Fog “tumbler,” as core proof in support of criminal forfeiture.¹⁴⁹ However, this admission did not occur automatically. The court relied on detailed expert testimony from government forensic analysts, who explained the technical operation of the blockchain system, methods for tracing transactions, and the integrity of the underlying data. The jury’s finding and the court’s ultimate ruling depended on both the technical chain of custody and the demonstration that the blockchain-derived evidence was “relevant and reliable” under the Federal Rules of Criminal Procedure and evidence law (see, e.g., Fed. R. Crim. P. 32.2(b); D.C. Cir. precedent).¹⁵⁰

Crucially, the *Sterlingov* decision underscores that US federal courts do not treat blockchain records as self-authenticating or presumptively admissible business records. Instead, their evidentiary value is determined on a case-by-case basis, requiring the proponent to establish the reliability, chain of custody, and probative value of the digital records through expert testimony and corroborative documentation.¹⁵¹ The court’s ruling reflects a broader judicial trend in the US: technical evidence from blockchain forensics is increasingly

¹⁴⁸ Jasperse, “50-State Review of Cryptocurrency and Blockchain Regulation.”

¹⁴⁹ Dadang Herli Saputra, and Fardana Kusumah. 2025. “Blockchain Forensics and the Evidentiary Challenges of Crypto-Based Corruption in Developing Countries”. *Indonesian Journal of Criminal Law Studies* 10 (2): 639. <https://doi.org/10.15294/ijcls.v10i2.28795>.

¹⁵⁰ Jasperse, “50-State Review of Cryptocurrency and Blockchain Regulation.”

¹⁵¹ Jasperse.

accepted, but only when robust, transparent, and well-documented methodologies are presented and subjected to adversarial scrutiny.

In contrast to the increasing acceptance of blockchain-based forensic evidence in some federal courts, *United States v. Larry Dean Harmon* demonstrates ongoing judicial reluctance to treat blockchain data as self-authenticating. Harmon operated “Helix,” a large-scale Bitcoin tumbler service used for laundering funds through the Darknet, and federal prosecutors relied heavily on blockchain analytics to trace flows of illicit cryptocurrency.¹⁵² However, during pretrial litigation, the court expressed concerns about the admissibility of blockchain analysis and transaction data absent robust expert testimony and independent validation.¹⁵³ The government was required to provide detailed authentication of the analytic tools, transparency of forensic methods, and a clear chain of custody before any blockchain records could be considered by the jury. Ultimately, significant portions of blockchain-derived evidence were excluded or heavily scrutinized precisely because the prosecution failed to offer sufficient corroboration or independent verification of the analytics used to link Harmon to the laundered funds.¹⁵⁴

This cautious approach underscores a persistent divide in US federal courts: while blockchain data can serve as valuable evidence, its admissibility depends on the proponent’s ability to demonstrate reliability, authenticity, and relevance through expert witnesses and supporting documentation. The Harmon case, thus, highlights judicial skepticism and the demand for strict evidentiary safeguards when introducing novel forms of digital evidence.

Across the European Union, the pursuit of legal certainty in blockchain applications is shaped by a complex interplay of primary legislation such as the eIDAS Regulation, Data Act, Markets in Crypto-Assets Regulation (MiCA), and the DLT Pilot Regime and cautious

¹⁵² *United States v. Harmon* (2021).

¹⁵³ *United States v. Harmon*, see also court orders on motions in limine and evidentiary hearings.

¹⁵⁴ *United States v. Harmon*, see also court orders on motions in limine and evidentiary hearings.

judicial practice at both national and Union levels.¹⁵⁵ While the eIDAS Regulation (EU No 910/2014, as amended by Regulation (EU) 2024/1183) establishes the legal basis for electronic ledgers as “electronic registered ledgers” and extends qualified trust services to include their issuance and management, as set out in Article 3(44a), Article 45b, and Article 45c.¹⁵⁶ The Data Act (Regulation (EU) 2023/2854) introduces horizontal rules on fair access to and use of data, as well as specific requirements for the auditability and termination of smart contracts used in data sharing agreements, as set out in Article 30 and Recital 104. The Data Act further complements the Data Governance Act, together establishing a harmonized framework to facilitate reliable and secure access to data and foster the creation of a single market for data in the EU, as highlighted in Recitals 1, 5, and 22.¹⁵⁷

Despite these regulatory advances, the translation of these frameworks into legal certainty for blockchain innovators remains uneven, particularly for cross-border projects where practical application is often complicated by divergent national interpretations and a lack of binding judicial precedent at the CJEU level.

These doctrinal and procedural uncertainties are made explicit in the European Blockchain Sandbox Best Practices Reports, a flagship initiative launched by the European Commission to facilitate confidential regulatory dialogues between innovators and both national and EU authorities.¹⁵⁸ For example, the 2024 Sandbox Report documents that digital identity pilots relying on self-sovereign blockchain solutions face ongoing interpretive challenges regarding the definition and regulatory status of a “qualified trust service” under eIDAS Article 3(16), as well as the application of the European Digital

¹⁵⁵ European Commission, “Blockchain and Web3 Strategy,” Shaping Europe’s Digital Future, 2025.

¹⁵⁶ Regulation EU, “Regulation (EU) 910/2014 as Amended by Regulation (EU) 2024/1183 on Establishing the European Digital Identity Framework,” 2024.

¹⁵⁷ Regulation EU, “Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data (Data Act),” 2023.

¹⁵⁸ European Commission, “European Blockchain Sandbox Best Practices Report, 2nd Cohort,” 2024 Recitals 1, 5, 22, 104 and Article 30.

Identity Wallet framework.¹⁵⁹ Despite regulatory advances, many national authorities remain cautious, requiring project developers to demonstrate compliance with both local KYC/AML requirements and Union-wide digital identity standards, often resulting in duplicative procedures and legal uncertainty for cross-border operability.¹⁶⁰

Similarly, while the Data Act's explicit regulation of smart contracts (Art. 30) has been welcomed as a doctrinal advance, project use cases discussed in the Sandbox reveal ongoing challenges.¹⁶¹ In particular, decentralized autonomous organizations (DAOs) and open-source smart contract deployments often struggle to meet the Act's requirements for manual override ("kill switch") and auditability, raising unresolved questions of enforceability and consumer protection in fully decentralized systems.¹⁶²

The Sandbox reports also highlight empirical lessons from ESG reporting and digital product passport projects, which leverage DLT for transparency and data integrity.¹⁶³ While these applications demonstrate the value of blockchain's immutability for regulatory compliance, they equally expose a fundamental limitation: the reliability of the system is only as strong as the data initially recorded. This is commonly described as the persistent "garbage in, garbage out" risk.¹⁶⁴ This problem is compounded by the need for robust interoperability between blockchain solutions and existing EU data governance frameworks, including the Data Governance Act and the Digital Services Act.¹⁶⁵

In the financial sector, regulatory clarity has been somewhat enhanced through the application of MiCA and the DLT Pilot

¹⁵⁹ European Commission.

¹⁶⁰ European Commission.

¹⁶¹ Regulation EU, "Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data (Data Act)."

¹⁶² European Commission, "European Blockchain Sandbox Best Practices Report, 2nd Cohort."

¹⁶³ European Commission.

¹⁶⁴ see Richard Sheposh, "Garbage in, Garbage out (GIGO)," EBSCO Research Starters: Computer Science, 2024; European Commission, "European Blockchain Sandbox Best Practices Report, 2nd Cohort."

¹⁶⁵ European Commission, "European Blockchain Sandbox Best Practices Report, 2nd Cohort"; Sheposh, "Garbage in, Garbage out (GIGO)."

Regime.¹⁶⁶ However, Sandbox dialogues (Sections 16–17, pp. 15–16) note that the classification of tokens and the application of financial market rules, such as the distinction between a security and a crypto-asset under MiFID II and MiCA, often vary between Member States.¹⁶⁷ This regulatory divergence is further reflected in the treatment of new market mechanisms, such as automated market makers, which are not yet uniformly addressed across all EU frameworks (Section 19).¹⁶⁸

Crucially, the Sandbox reports underscore that, notwithstanding legislative progress and increased regulatory engagement, the probative value and legal admissibility of blockchain evidence and smart contracts remain subject to the ultimate discretion of national courts and competent authorities. As a result, the pursuit of legal certainty for blockchain applications in the EU remains an ongoing, iterative process, one that depends as much on continued regulatory dialogue and the development of sector-specific best practices as it does on statutory reform.¹⁶⁹

On the other hand, China and Singapore have made blockchain a key part of their legal systems for enforcing intellectual property (IP) and digital rights. Since 2018, Chinese Internet Courts have formally recognized and admitted blockchain-stored data as key evidence in disputes involving copyright, online platforms, and algorithmic transactions. The Provisions of the Supreme People’s Court on the Trial of Cases by Internet Courts, especially Article 11, back this practice. Article 11 says that electronic evidence can be verified using technical methods like hash value checks and trusted timestamps. In judicial proceedings, the courts presume the authenticity of blockchain evidence if it is technically consistent, unique, and has not been contradicted by other evidence, thus enabling a more reliable verification and preservation process for digital rights claims.¹⁷⁰ In landmark cases, the

¹⁶⁶ Regulation EU, “Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA),” 2023.

¹⁶⁷ European Commission, “European Blockchain Sandbox Best Practices Report, 2nd Cohort.”

¹⁶⁸ European Commission.

¹⁶⁹ European Commission.

¹⁷⁰ Tian Lu, “The Implementation of Blockchain Technologies in Chinese Courts,” *Stanford Journal of Blockchain Law & Policy* 4 (2021).

Beijing Internet Court has repeatedly upheld copyright claims where the creation process and original work were recorded and notarized on blockchain platforms, confirming such digital evidence as credible and tamper-proof.¹⁷¹ This framework is further supported by recent research that demonstrates that China's three major Internet Courts, Beijing, Hangzhou, and Guangzhou have institutionalized blockchain-based schemes for judicial evidence preservation. For example, the Hangzhou Internet judicial blockchain handled more than 640,000 evidence storage and invocation operations within three and a half months of launch in 2018, while Beijing's "Tian-Ping Chain" stored over 187,000 evidence items in just three months. These systems leverage blockchain's immutability, hash verification, and trusted timestamps to guarantee the integrity and authenticity of digital evidence, with tested throughputs exceeding 300 transactions per second in major cities, and are now integral to the efficiency and reliability of digital rights enforcement in Chinese Internet Courts.¹⁷²

At the same time, the evidentiary strength of blockchain infrastructure remains structurally bounded by the quality and legality of the underlying inputs. Blockchain-based timestamps can confirm that a record existed at a particular moment, but they do not verify the truthfulness, legality, or authorship of the content recorded. When registering infringing or misattributed works on-chain, immutability may reinforce rather than rectify errors. This "Garbage In, Garbage Out" limitation underscores that blockchain enhances procedural reliability without resolving substantive questions of copyright compliance, lawful data sourcing, or creative attribution—functions that remain dependent on off-chain verification and institutional oversight.

Meanwhile, Singapore's regulatory environment is anchored by the Financial Services and Markets Act 2022 and the MAS FinTech Regulatory Sandbox Guidelines, which expressly allow innovative solutions, including blockchain-based rights management, tokenized assets, and legaltech applications, to be piloted under regulatory

¹⁷¹ Beijing Internet Court, "Top Ten Typical Cases in Five Categories," 2023.

¹⁷² Shuaiqi Liu and Qingxiao Zheng, "A Study of a Blockchain-Based Judicial Evidence Preservation Scheme," *Blockchain: Research and Applications* 5, no. 2 (2024): 100192, <https://doi.org/10.1016/j.bcra.2024.100192>.

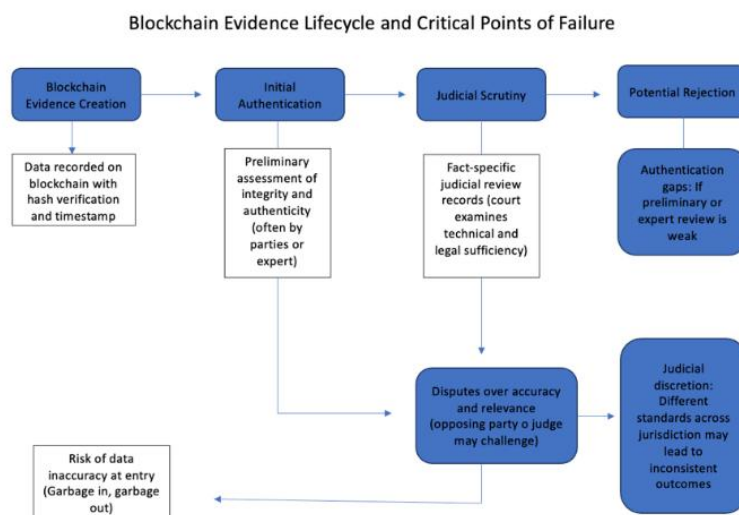
oversight.¹⁷³ According to the State of Legal Innovation in the Asia Pacific report, Singapore's Future Law Innovation Programme (FLIP), including its regulatory sandbox, has enabled law firms, in-house legal teams, and legal technology providers to pilot solutions for e-discovery, e-evidence, smart contract deployment, and digital authentication in a safe, supervised environment, thereby accelerating adoption and regulatory clarity for new models of legal service delivery.¹⁷⁴ Across ASEAN, pilot projects for NFT registries and digital authentication schemes suggest a growing willingness to experiment with blockchain-backed IP infrastructure, but standards for interoperability and cross-border legal recognition remain unsettled.¹⁷⁵

Figure 1 below presents the blockchain evidence lifecycle, mapping out each critical point at which data accuracy or legal validation may fail from the moment data is entered onto the blockchain to its final scrutiny and potential rejection in court. The diagram makes clear that technical immutability is no substitute for careful legal assessment at every stage, especially where off-chain assets or issues of human identification are at stake.

¹⁷³ Attorney-General's Chambers of Singapore, "Financial Services and Markets Act 2022 (No. 18 of 2022)," 2022; Monetary Authority of Singapore, "FinTech Regulatory Sandbox Guidelines," 2022.

¹⁷⁴ Jerrold Soh, Josh Kok Tong Lee, and Felix Tan, "State of Legal Innovation in the Asia Pacific," 2019, 118–19.

¹⁷⁵ Soh, Lee, and Tan, "State of Legal Innovation in the Asia Pacific."

Figure 1. Blockchain Evidence Lifecycle and Critical Points of Failure

Source: Compiled and adapted by the author from WIPO, Blockchain Evidence Report (2025), OECD.

Despite these technical and institutional advances, fundamental limitations persist. The “garbage in, garbage out” problem explicitly analyzed by legal scholars such as De Filippi and Wright highlights that, without institutional oversight, errors or misattribution at the data entry stage become permanently embedded and uncorrectable on the blockchain, undermining the reliability of blockchain-based registries.¹⁷⁶ Courts, even in jurisdictions that support digital evidence, are rarely willing to treat ledger entries as fully self-proving, instead requiring expert testimony and a demonstrable link between the digital record and a verifiable legal subject.¹⁷⁷ For off-chain assets such as NFT-linked artwork, creative content, or AI-generated outputs, the evidentiary value of blockchain records ultimately hinges on whether the relevant legal regime recognizes the underlying authorship and ownership claims. As

¹⁷⁶ Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press, 2018), 114–15.

¹⁷⁷ Xukang Wang, Ying Cheng Wu, and Zhe Ma, “Blockchain in the Courtroom: Exploring Its Evidentiary Significance and Procedural Implications in U.S. Judicial Processes,” *Frontiers in Blockchain* 7 (2024): 4, <https://doi.org/10.3389/fbloc.2024.1306058>.

De Filippi and Wright emphasize, blockchain provides an immutable and transparent proof of record, but legal enforceability depends on external attribution and the acceptance of such records by courts or regulatory authorities. Thus, for any asset whose legal status is not natively defined on-chain, the role of blockchain evidence is secondary to, and contingent upon, the surrounding legal framework regarding rights attribution and ownership.¹⁷⁸

Importantly, the distribution of benefits from blockchain-based evidence remains highly uneven. Access to advanced verification mechanisms such as blockchain notary services or digital courts is often restricted to well-resourced actors and technologically advanced jurisdictions, while creators in the Global South and less-developed markets are left with greater evidentiary uncertainty and far fewer practical remedies.¹⁷⁹ Even when advanced technical solutions like blockchain platforms exist, factors such as high transaction costs, technical complexity, and disparities in digital skills or platform governance can still effectively exclude less-resourced and marginalized creators from fully accessing justice or asserting their rights, as they are unable to overcome the economic and technological barriers built into these systems.¹⁸⁰ As legal scholar Rebecca Berto has emphasized, the reliability of blockchain evidence in court depends not only on the technical strength of cryptographic safeguards but also on the accuracy and integrity of data entry and the court's ability to interpret the technology. If mistakes or manipulation occur at the data entry stage, the immutable nature of blockchain means such errors become permanent, rendering all technical guarantees ineffective for the purpose of proof.¹⁸¹ As the OECD (2021) notes, the rapid digital transformation, while promising broad benefits, has in practice often deepened existing inequalities between firms, individuals, and regions. The advantages of digitalization, including blockchain and other 'trustless' technologies,

¹⁷⁸ Filippi and Wright, *Blockchain and the Law: The Rule of Code*.

¹⁷⁹ Raúl Zambrano, "Taming the Beast: Harnessing Blockchains in Developing Country Governments," *Frontiers in Blockchain* Volume 2- (2020), <https://doi.org/10.3389/fbloc.2019.00027>.

¹⁸⁰ Filippi and Wright, *Blockchain and the Law: The Rule of Code*.

¹⁸¹ Rebecca Berto, "Blockchain Records: Is the Evidence Admissible? A Challenge for European Member States," *Civil Procedure Review* 10, no. 3 (2019).

tend to be captured by early adopters and well-resourced actors, thereby reinforcing pre-existing hierarchies and digital divides, rather than ensuring equitable outcomes for all.¹⁸²

In conclusion, blockchain has the potential to change the way evidence is used, but it still can't provide real legal certainty because of jurisdictional limits, socio-economic barriers, and the fact that doctrinal ambiguity is still present. This underscores the need for further policy attention and legal innovation to ensure that advances in digital evidence do not merely automate existing inequalities but instead support broad-based access to justice, effective remedies, and the equitable recognition of creative rights. Policy reforms should prioritize the harmonization of evidentiary standards for blockchain records, investment in digital legal infrastructure for underserved jurisdictions, and the development of clear protocols for linking on-chain evidence to off-chain legal identities and rights. This could include cross-border recognition agreements, public legal tech education, and institutional support for digital notary and dispute resolution systems.

D. Programmable Rights and the Legal Uncertainty of Automated Royalties

In recent years, the concept of the “smart contract,” self-executing agreements whose terms are encoded and deployed on a blockchain, executing automatically when predetermined conditions are met, has evolved from a technical innovation into a subject of growing relevance within legal, economic, and creative industries.¹⁸³ Fundamentally, a smart contract is a piece of computer code residing on a decentralized blockchain network, programmed to autonomously enforce the rights and obligations of contracting parties.¹⁸⁴ This marks a substantial shift from conventional legal contracts, which depend on manual

¹⁸² Organisation for Economic Co-operation and Development (OECD), “The Digital Transformation of SMEs,” 2021, 17, 162–63.

¹⁸³ Natália Tavares Borges and Rui Pedro Rodrigues Leite, “Revolutionizing Contracts: The Impact of Blockchain Technology and Smart Contracts,” *JustGov Research Paper No 2024-23*, 2024, 1–2, <https://doi.org/10.2139/ssrn.5064863>.

¹⁸⁴ Borges and Leite, “Revolutionizing Contracts: The Impact of Blockchain Technology and Smart Contracts.”

enforcement and third-party institutions; smart contracts instead operate “trustlessly,” reducing the need for centralized arbiters and enhancing transparency through immutable public ledgers.¹⁸⁵

The increasing sophistication of public blockchains, especially Ethereum, has broadened the role of smart contracts from simple asset transfers to tools for embedding complex legal and economic rights within digital assets.¹⁸⁶ For example, the ERC-2981 standard, an Ethereum blockchain protocol, enables NFT creators to receive automatic royalty payments from secondary sales.¹⁸⁷ In practice, NFT smart contracts, when built on protocols such as ERC-2981, fundamentally change the way artists monetize and control their digital creations. The technical standard allows creators to embed royalty instructions directly into NFT metadata at the time of minting, specifying the percentage of each resale to be automatically allocated to the original artist or designated recipients.¹⁸⁸ This royalty logic becomes an inseparable part of the NFT’s code, enabling on-chain enforcement of payment terms provided the secondary marketplace supports the royalty standard in its smart contract architecture.¹⁸⁹

From a technical point of view, ERC-2981 sets a standard way for NFT contracts to send information about royalty payments. At the point of sale, marketplaces can query the royalty info function, which returns both the designated royalty recipient address and the royalty amount as a percentage of the sale price. However, ERC-2981 is technically limited to a single recipient per NFT, and crucially, enforcement is not on-chain but dependent on whether marketplaces choose to implement the royalty logic in their own codebase. Thus, while royalty splits can be codified on-chain, actual payment remains partly off-chain unless marketplaces implement and respect the standard.¹⁹⁰

¹⁸⁵ Filipi and Wright, *Blockchain and the Law: The Rule of Code*.

¹⁸⁶ Filipi and Wright.

¹⁸⁷ Kristaps Grinbergs, “Implementing the ERC-2981 NFT Royalty Standard with Solidity - a Game-Changer for Creators to Receive Income from Every Sale,” DEV Community, 2023.

¹⁸⁸ Grinbergs.

¹⁸⁹ Grinbergs.

¹⁹⁰ Inc Artema Labs, “Systems and Methods for Facilitating Access to Token Content, Patent US20230385815A1, Issued May 24, 2023,” 2023.

For collaborative or partial-AI works, advanced smart contract protocols such as 0xSplits (also known as OsSplits) are now being adopted to enable true on-chain, trustless distribution of royalties among multiple parties. Instead of specifying a single royalty recipient, 0xSplits contracts can programmatically route payments to any number of addresses and customizable percentages. This approach is particularly relevant for hybrid NFT projects involving human artists, AI model developers, and even platform coders, ensuring all stakeholders, including AI tool providers, receive their fair share in real time at each secondary sale, regardless of individual marketplace compliance with ERC-2981.¹⁹¹

This technical architecture is exemplified in hybrid NFT projects such as Kusano's AI-generated art, where payout logic may allocate 50% of royalties to the human artist, 30% to the AI model provider, and 20% to the creative coder. Using OsSplits, these distributions are executed atomically on-chain for every secondary sale, with the smart contract guaranteeing programmable, auditable, and irreversible revenue sharing among all contributors. Such mechanisms support new forms of collaborative creative production by embedding multi-party revenue-sharing logic at the protocol level.¹⁹²

Despite advances in programmable royalty logic, vulnerabilities persist, most notably the risk of "royalty bypass," where off-chain or non-compliant marketplace transfers evade payment obligations. Recent advancements in wrapper contracts and enforcement protocols, such as mandatory use of royalty enforcement wrappers, seek to address this by requiring all secondary sales to be routed through contracts that verify and enforce royalty splits before the transfer of ownership is finalized. This development marks a significant step toward protocol-level guarantees for creator compensation, even as some platforms experiment with "zero royalty" policies or intermittent disabling of enforced royalties.¹⁹³

In practice, as documented in both market analysis and industry commentary, the effectiveness of this model depends on each

¹⁹¹ Inc Artema Labs.

¹⁹² Inc Artema Labs.

¹⁹³ Inc Artema Labs.

marketplace's commitment to respecting on-chain royalty logic. As shown in recent studies, major platforms such as OpenSea, SuperRare, LooksRare, Blur, and Foundation have implemented ERC-2981 and related royalty standards, allowing creators to list NFTs with embedded royalty rules and—where supported—receive automated payments for each resale event. This system not only enhances transparency and accountability but also dramatically reduces the scope for disputes between artists and buyers, since payout and royalty percentages are written into code rather than dependent on ad hoc platform policy.¹⁹⁴

However, recent quarterly NFT market reports reveal that real-world outcomes remain uneven. Throughout 2022, the proportion of sales where royalties are actually paid out varied significantly due to inconsistent platform support and buyer behavior. For example, some sales occur “off-chain” or via marketplaces that do not honor ERC-2981 metadata, allowing royalties to be bypassed.¹⁹⁵ This results in a fragmented compensation landscape, where artists benefit most in ecosystems with robust, enforceable royalty compliance but remain exposed to revenue loss when marketplaces or collectors opt out of the protocol. A comparative analysis of royalty enforcement and payout mechanisms across leading NFT marketplaces reveals substantial variation in technical standards, protocol compliance, and the degree of protection afforded to creators.¹⁹⁶

¹⁹⁴ Li Ruiqiang et al., “Empowering Visual Artists with Tokenized Digital Assets with NFTs,” 2024.

¹⁹⁵ Inc Artema Labs, “Systems and Methods for Facilitating Access to Token Content, Patent US20230385815A1, Issued May 24, 2023.”

¹⁹⁶ Inc Artema Labs.

Table 2. Comparative enforcement of NFT royalties across major marketplaces (2023–2024).

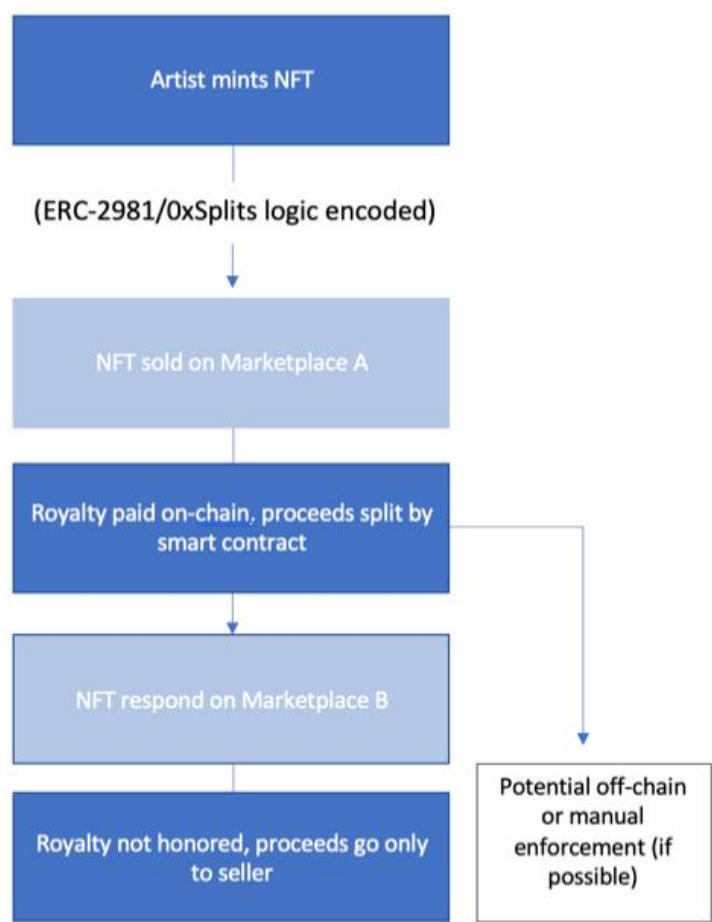
Marketplace	ERC-2981 Support	Off-chain Bypass Possible	Programmable Splits	Royalty Escrow	Payout Rate
OpenSea	Yes/Partial	Yes	Yes	No	70-80%
SuperRare	Yes	No	Yes	Yes	~100%
Blur	Partial/No	Yes	No	No	40-60%
Foundation	Yes	No	Yes	Yes	90-95%
LooksRare	No	Yes	No	No	<50%

Sources: NFTGo (2024), Galaxy Digital (2023), OpenSea Docs, SuperRare Docs, and marketplace policies.

Still, the rise of on-chain programmable royalties is a big step forward from older digital art models. The ability to codify and automate creator compensation on the blockchain offers a pathway to ongoing income and greater economic agency for artists, provided that legal, technical, and platform-level standards continue to converge in support of transparent, fair digital art markets. This model eliminates the need for off-chain monitoring or intermediary enforcement; royalty terms are written directly into the NFT’s code, so each time a secondary sale occurs on a compatible marketplace, a portion of the proceeds is automatically distributed to the original creator’s wallet. However, this automated process relies on the technical compliance of each marketplace and may be circumvented in non-compliant or off-chain sales scenarios, as detailed in recent protocol and patent literature. The following diagram illustrates the operational differences between automated, on-chain royalty enforcement and manual, off-chain payout processes across NFT marketplaces.¹⁹⁷

¹⁹⁷ Inc Artema Labs.

Figure 2. Automated versus manual royalty enforcement in NFT smart contract transactions.



Source: Authors' own elaboration

Automated revenue distribution protocols such as 0xSplits exemplify how programmable smart contracts enable the programmatic division of incoming payments among multiple parties, transparently and without the need for off-chain coordination.¹⁹⁸ By directly specifying

¹⁹⁸ Laura Lotti, Nick Houde, and Tara Merk, "Social Security for Web3 Work: A Preliminary Specification of the Design and Deployment of Solidarity Primitives

revenue splits within the contract, platforms can distribute NFT sales, licensing fees, or other digital asset revenues among all contributors according to predefined ratios, ensuring on-chain, auditable allocation.¹⁹⁹ As documented in recent web3 labor research, such “solidarity primitives” now underpin a range of automated payout models, including vesting contracts, contract-secured revenue (CSR), and UBI streams that address both the technical and social dimensions of financial security for DAO contributors.²⁰⁰ These mechanisms have been widely adopted to automate collective payouts and enforce royalty distribution, a model now being extended to collaborative NFT and AI-driven art projects, where artists, coders, and even AI model owners can all receive their share instantly, algorithmically, and without intermediary intervention.²⁰¹ By embedding automated, transparent compensation at the protocol level, programmable contracts have become a foundational tool for multi-party royalty management and collective welfare across the digital creative economy.²⁰²

Simultaneously, Decentralized Autonomous Organizations (DAOs) which are collectives managed by smart contracts and governed by on-chain voting, are emerging as new models for digital rights and revenue governance. Within a DAO, the rules for allocating royalties, licensing income, or governance rights are encoded transparently in smart contracts, allowing token holders to participate in decision-making and administration without traditional managerial hierarchies.²⁰³

Taken together, these innovations are fundamentally reshaping digital rights management by embedding legal, economic, and governance mechanisms directly into the technical architecture of digital assets. While such approaches offer the potential to reduce friction,

for DAO Contributors,” *SSRN Electronic Journal*, no. July (2023): 1–2, <https://doi.org/10.2139/ssrn.4596552>.

¹⁹⁹ Lotti, Houde, and Merk, “Social Security for Web3 Work: A Preliminary Specification of the Design and Deployment of Solidarity Primitives for DAO Contributors.”

²⁰⁰ Lotti, Houde, and Merk.

²⁰¹ Lotti, Houde, and Merk.

²⁰² Lotti, Houde, and Merk.

²⁰³ Benjamin Nemeroff, “Understanding Decentralized Autonomous Organizations I Nym,” Nym, 2025.

improve transparency, and expand economic opportunities for creators, they also introduce doctrinal and distributive challenges.²⁰⁴ The increasing reliance on “code as law,” a concept popularized by Lawrence Lessig raises unresolved issues regarding legal enforceability, inclusion, and the risk that those who design or control the underlying code may inadvertently (or intentionally) embed new forms of exclusion or bias.²⁰⁵

By the end of 2022, total royalty payments to creators on the Ethereum blockchain surpassed \$1.8 billion, but studies (Qadir & Parker, 2022) also show that enforcement depends almost entirely on marketplace policy, not just ERC-2981 compliance at the smart contract level.²⁰⁶ While ERC-2981 is the main standard on Ethereum, cross-chain royalty standards are also in development (e.g., EIP-4907 for rentals, Solana’s and Polygon’s native royalty standards), but interoperability remains a problem; royalty instructions are often lost when NFTs are bridged between blockchains.²⁰⁷ Platforms like Manifold and Zora now let creators dynamically configure royalty percentages, set tiered royalty models, or create time-limited royalty rules (for example, 10% for the first year, then 2% thereafter). On Manifold, creators can use built-in split contracts to allocate royalties across multiple recipients and update them over time, while on Zora, artists can enforce resale royalties and configure payout structures directly within the platform’s smart contracts.²⁰⁸ This degree of programmability and flexibility enhances creator autonomy and income certainty, although it also increases technical and contractual complexity for both creators and collectors.²⁰⁹ NFTs are unique digital assets that enable visual artists to transform their works, such as artwork, music, or collectibles, into verifiable blockchain tokens through a process known as minting. According to Li et al., the typical workflow involves first creating a digital asset, then minting it as an NFT on a compatible blockchain platform (e.g., Ethereum), after which the artist lists the NFT

²⁰⁴ Nemeroff.

²⁰⁵ Lessig, *Code and Other Laws of Cyberspace*.

²⁰⁶ S. Qadir and G. Parker, “NFT Royalties: The \$1.8bn Question,” *Galaxy*, 2022.

²⁰⁷ Lance Anders and Shrug, “ERC-4907: Rental NFT, an Extension of EIP-721,” 2022; Ruiqiang et al., “Empowering Visual Artists with Tokenized Digital Assets with NFTs.”

²⁰⁸ Splits Help Center, “Using Manifold with Splits,” Splits, 2024.

²⁰⁹ Gate.com, “Zora: Redefining Value in Digital Art,” 2024.

smart contract on a marketplace such as OpenSea, Rarible, or Foundation. Upon minting, ownership and transaction records are transparently logged on-chain, and self-executing NFT smart contracts can ensure that creators receive royalties from subsequent resales. This streamlined process allows artists to directly access global markets and benefit from automated, code-based compensation systems.²¹⁰

Fragmented marketplace policies mean NFT royalty enforcement is rarely guaranteed by code alone; rather, creator payouts remain highly dependent on the willingness of each platform or buyer to honor them. In the absence of harmonized frameworks or mandatory marketplace rules, artists, including those in less-resourced regions, face persistent uncertainty about whether smart contract royalties will actually be paid.²¹¹

Technical complexity increases further in collaborative projects, such as partial AI-generated art, where transparent and granular value distribution is critical. Protocols like 0xSplits, introduced in 2023, enable programmatic allocation of revenue among multiple stakeholders, reducing manual errors and intra-project disputes.²¹² Nonetheless, as with ERC-2981, effectiveness is hampered by limited cross-platform adoption and technical fragmentation: revenue can be rerouted or lost if even one link in the ecosystem is non-compliant.²¹³

Smart contract audits are critical: recent exploits include reentrancy bugs and royalty payout address manipulations.²¹⁴ Marketplace fraud such as “fee evasion” and delayed royalty payouts has prompted some visual art DAOs (e.g., The Mint Fund, Foundation) to implement on-chain escrow models for royalty protection.²¹⁵ Common vulnerabilities include phishing, metadata tampering, and marketplace

²¹⁰ Ruiqiang et al., “Empowering Visual Artists with Tokenized Digital Assets with NFTs.”

²¹¹ Emily Ekshian, “How NFT Royalties Work - and Sometimes Don’t,” Crypto Council for Innovation, 2023.

²¹² Splits Help Center, “Using Manifold with Splits.”

²¹³ Ruiqiang et al., “Empowering Visual Artists with Tokenized Digital Assets with NFTs.”

²¹⁴ Consensys Diligence, “Smart Contract Audits,” 2025.

²¹⁵ Giacomo Bertazzolo, “NFTs in the Digital Age: Cybersecurity Risks and AI-Powered Smart Contract Solution,” 2023, 36–37, 47, 57–58.

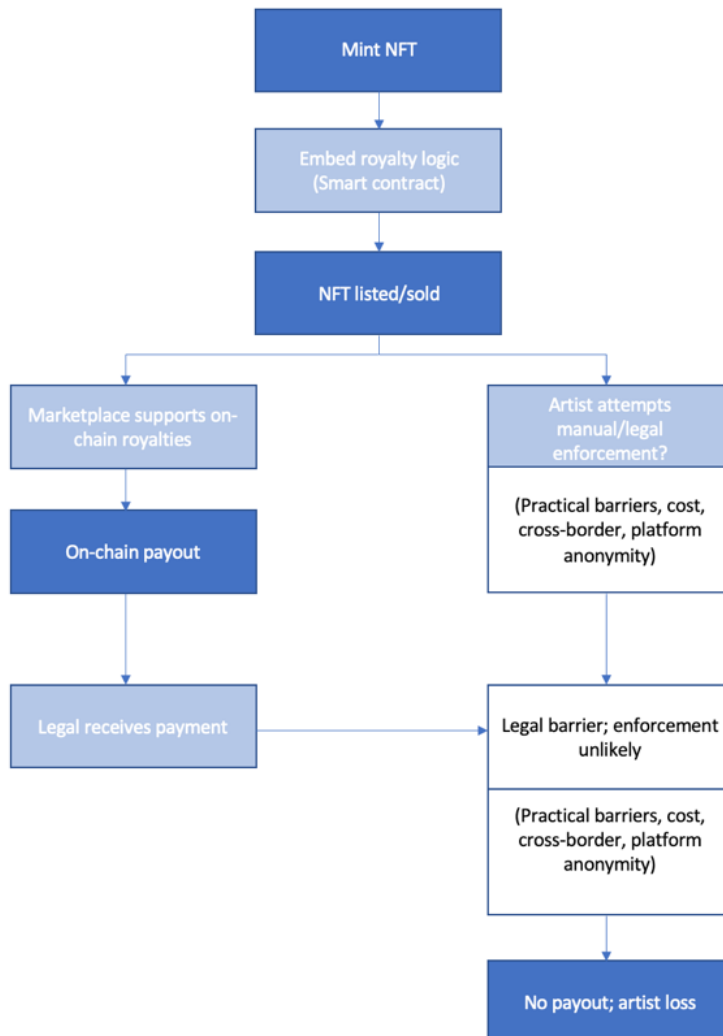
fee evasion.²¹⁶ Notably, on many platforms, sellers can bypass royalty payments by conducting off-platform transfers or exploiting differences in royalty enforcement across marketplaces, exposing artists to further revenue loss.²¹⁷ As a result, platforms like Foundation rely on on-chain escrow and mandatory verification to reduce manipulation and ensure fair distribution of royalties.²¹⁸ Enhanced smart contract auditing and transparent transaction records remain crucial to protecting both artists and collectors in this rapidly evolving landscape. The following decision tree outlines the intersecting legal and technical pathways that determine how NFT royalty payments are enforced or denied across various transaction scenarios. The following decision tree outlines the intersecting legal and technical pathways that determine how NFT royalty payments are enforced or denied across various transaction scenarios.

²¹⁶ Bertazzolo, “NFTs in the Digital Age: Cybersecurity Risks and AI-Powered Smart Contract Solution.”

²¹⁷ Bertazzolo.

²¹⁸ Bertazzolo.

Figure 3. Decision Tree Illustrating Legal and Technical Failure Points in NFT Royalty Enforcement



Source: Adapted from Giacomo Bertacuzza, “NFTs in the Digital Age: Cybersecurity Risks and AI-Powered Smart Contract Solution” (Università di Pisa, 2023), 47, 57–58.

At the legal level, the enforceability of smart contracts for NFT royalties remains highly fragmented. In the United States, the legal enforceability of smart contracts rests on a robust framework for electronic signatures, consisting primarily of the Electronic Signatures in

Global and National Commerce (ESIGN) Act and the Uniform Electronic Transactions Act (UETA).²¹⁹ The Electronic Signatures in Global and National Commerce (ESIGN) Act grants electronic signatures, including a broad range of electronic processes, such as email authentication, PIN entry, or click-to-accept, the same legal status as handwritten signatures, provided that the parties clearly intend to sign, consent to transact electronically, and the electronic record is retained and accessible for later reference.²²⁰ Before giving consent, consumers must receive a clear and conspicuous statement of their rights to receive paper copies, the procedures for withdrawing consent, and the hardware and software requirements for access and retention of electronic records. Consent must be given electronically, in a way that reasonably demonstrates the consumer's ability to access information in the intended format.²²¹ The ESIGN Act excludes certain categories of documents, such as wills, testamentary trusts, and vital records from coverage and specifies that oral communications or recordings do not qualify as electronic records. Financial institutions and businesses must maintain accurate electronic records that are accessible and reproducible for all parties legally entitled to access them for the duration required by law.²²²

UETA, which has been adopted by 49 states, provides that “[a] record or signature may not be denied legal effect or enforceability solely because it is in electronic form,” and that “[i]f a law requires a record to be in writing, an electronic record satisfies the law.”²²³ This legal recognition is codified in Section 7(a)–(d) of the Uniform Electronic Transactions Act (UETA), making clear that electronic records, signatures, and contracts are fully enforceable so long as other substantive legal requirements are met.²²⁴ At the same time, Section 3(b) expressly

²¹⁹ U.S. Government Printing Office, “Electronic Signatures in Global and National Commerce Act, Pub. L. Public Law 106–229, 15 U.S.C. § 7001 et Seq.,” 2000; Uniform Laws, “Uniform Electronic Transactions Act, Pub. L. ULC 1999,” 1999.

²²⁰ U.S. Government Printing Office, “Electronic Signatures in Global and National Commerce Act, Pub. L. Public Law 106–229, 15 U.S.C. § 7001 et Seq.”

²²¹ U.S. Government Printing Office.

²²² U.S. Government Printing Office.

²²³ Uniform Laws, “Uniform Electronic Transactions Act, Pub. L. ULC 1999.”

²²⁴ Uniform Laws.

excludes certain transactions from UETA's scope, including any governed by laws on the creation and execution of wills, codicils, or testamentary trusts.²²⁵ As a result, while electronic agreements are generally accepted in commercial contexts, specific document types remain subject to traditional formalities and are not covered by the Act.²²⁶

While New York's Electronic Signatures and Records Act (ESRA) establishes a regime parallel to UETA, its legal foundation is codified in Article III of the State Technology Law (§§301–309).²²⁷ Under ESRA, electronic signatures are expressly afforded “the same validity and effect as the use of a signature affixed by hand” (§304[2]),²²⁸ while electronic records are recognized to have “the same force and effect as those records not produced by electronic means” (§305[3]).²²⁹ A key distinction from UETA lies in the designation of the Office of Information Technology Services (ITS) as the electronic facilitator (§303),²³⁰ which is charged with developing, coordinating, and enforcing statewide policy on electronic signatures and records.

This statutory framework is operationalized through detailed administrative regulations in Title 9 NYCRR Part 540, which implement ESRA's core principles in a manner that is both comprehensive and technologically neutral. The regulations require, among other things, that governmental entities conduct documented risk assessments before adopting any electronic signature solution (§540.4(c)).²³¹ They also mandate the legal equivalence of electronic signatures and records with their handwritten and paper counterparts, as reflected in §§540.1 and 540.4(a),²³² ensuring that digital processes are treated with the same legal weight as traditional methods. Furthermore, Part 540 establishes rigorous standards for privacy, authenticity, and the

²²⁵ Uniform Laws.

²²⁶ Uniform Laws.

²²⁷ N.Y. State Technology Law, “N.Y. State Technology Law -Art. III,” 2016, §§301–309.

²²⁸ N.Y. State Technology Law, “N.Y. State Technology Law -Art. III.”

²²⁹ N.Y. State Technology Law.

²³⁰ N.Y. State Technology Law.

²³¹ N.Y. Office of Information Technology Services, “Electronic Signatures and Records,” 2023, Title 9 NYCRR Part 540, §540.4(c).

²³² N.Y. Office of Information Technology Services, “Electronic Signatures and Records.”

preservation of electronic records over their full lifecycle, as outlined in §§540.5, 540.6, and 540.7.²³³ These rules are intentionally flexible and technology-neutral, expressly accommodating new innovations—including blockchain-secured signatures and smart contracts—so long as they satisfy ESRA’s statutory requirements and implementing regulations.²³⁴

Reflecting these developments, a number of U.S. states, such as Arizona, Nevada, and Tennessee have amended their statutes to explicitly include blockchain-based signatures and smart contracts as legally valid electronic records and signatures.²³⁵ As a result, except for categories expressly excluded by statute, smart contracts and blockchain-based agreements are legally recognized as enforceable contracts under both federal and most state laws, provided that the traditional elements of contract formation, including intent, mutual consent, and record retention, are satisfied.²³⁶

In the European Union, the eIDAS Regulation provides a comprehensive, three-tier regime for electronic signatures: simple, advanced, and qualified, each offering progressively higher standards of security, reliability, and legal certainty.²³⁷ Although the regulation does not expressly mention “smart contracts,” its framework is intentionally technology-neutral, ensuring that any electronic signature mechanism, including those implemented via automated or self-executing code, may be legally valid if it fulfills the applicable requirements.²³⁸ Under Article 25, an electronic signature “shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form,” and a qualified electronic signature carries the same legal effect as a handwritten signature throughout all EU Member

²³³ N.Y. Office of Information Technology Services.

²³⁴ N.Y. Office of Information Technology Services.

²³⁵ Jasperse, “50-State Review of Cryptocurrency and Blockchain Regulation.”

²³⁶ Jasperse.

²³⁷ Regulation EU, “Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation),” 2014, Recital 27, Art. 3(10)–(12).

²³⁸ Regulation EU, “Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation).”

States.²³⁹ The technical and legal criteria for advanced and qualified electronic signatures are further defined in Articles 3, 26, and Annexes I–III, which set requirements for signatory identification, data integrity, and certificate-based trust.²⁴⁰ As a result, smart contracts that incorporate an electronic signature mechanism compliant with eIDAS standards, particularly at the advanced or qualified level, can serve as legally valid signatures or instruments, provided that they satisfy the core elements of authenticity, signatory intent, and record integrity.²⁴¹ This approach ensures that the legal recognition of smart contracts under EU law depends not on their form, but on their compliance with substantive requirements for electronic signatures as established by eIDAS.

While Asian jurisdictions have begun to incorporate smart contract recognition into their legal systems, the path and substance of regulation are far from uniform. This discussion focuses on the Singapore, Malaysia, India, and China jurisdictions that are widely regarded as the frontiers of smart contract regulation and adoption in Asia. These countries exemplify the diversity of legal systems and policy approaches in the region and offer particularly illustrative insights into the evolving landscape of smart contract governance. Singapore is included in this analysis as it stands out as a clear leader in the regulation and judicial recognition of smart contracts in Asia. The country has developed advanced legislative frameworks and a growing body of case law that provide legal certainty and practical guidance for both industry and regulators. Singapore stands out with its Electronic Transactions Act 2010, where Section 7 explicitly states that any statutory requirement for writing or signature can be fulfilled electronically.²⁴² This legislative framework was designed not only to facilitate traditional e-commerce but also to accommodate the increasing automation of agreements via smart contract code. In real-world application, however, the legal enforceability of smart contracts in Singapore is not absolute and depends on the specific characteristics of each contract.

²³⁹ Regulation EU.

²⁴⁰ Regulation EU.

²⁴¹ Regulation EU.

²⁴² Singapore Statutes Online, “Electronic Transactions Act 2010,” 2010.

As explained in local legal guidance, smart contracts are generally considered legally binding so long as they fulfill the basic elements of contract law: offer, acceptance, intention to create legal relations, and consideration. Nonetheless, Singaporean courts have yet to definitively rule on the enforceability of smart contracts that are written purely in code, and each contract must be assessed individually to determine its legal effect. For certain transactions that require statutory formalities, such as contracts for the sale of property, hire-purchase agreements, or the transfer of ships, there remains uncertainty as to whether a code-only smart contract would meet requirements for writing and signature. Moreover, where the contract contains illegal terms or was made under duress, or where parties expressly exclude legal enforceability, Singapore law may still intervene to deny recognition or enforcement. Thus, while the ETA 2010 provides robust support for the use of smart contracts, their enforceability in practice is determined on a case-by-case basis in accordance with underlying principles of contract law and statutory formality requirements.²⁴³

Building on Singapore's position as a regional benchmark, Malaysia represents an emerging jurisdiction that is actively developing its regulatory framework for smart contracts.²⁴⁴ The Electronic Commerce Act 2006, modelled on the UNCITRAL Model Law on Electronic Commerce 1996, constitutes the primary statutory basis for smart contracts. Sections 6 and 7 of the ECA 2006 explicitly provide that electronic messages, including those forming the basis of a contract, are not to be denied legal effect, validity, or enforceability solely by reason of their electronic form. The Act further recognises electronic signatures, thereby allowing digital keys or tokens in blockchain transactions to serve as valid signatures for contractual purposes under Malaysian law.²⁴⁵

In practice, legal commentaries such as those by Shin Associates observe that the enforceability of smart contracts in Malaysia generally follows traditional principles of contract law. Provided that the essential

²⁴³ Singapore Legal Advice, "Using Smart Contracts in Singapore: Benefits and Risks," 2024.

²⁴⁴ United Nations Commission on International Trade Law, "UNCITRAL Model Law on Electronic Commerce (1996) with Additional Article 5 Bis as Adopted in 1998," 1996.

²⁴⁵ Electronic Commerce Act, "Laws of Malaysia," 2006, Part II, Sections 6–7.

elements of offer, acceptance, consideration, and intention to create legal relations are fulfilled, smart contracts may be considered valid and enforceable.²⁴⁶ Nevertheless, challenges persist, particularly in relation to statutory formalities such as notarisation or stamping for court admissibility, which may impede the enforcement of blockchain-based agreements. Standard vitiating factors, including fraud, illegality, and incapacity, remain applicable irrespective of technological medium.²⁴⁷ Thus, although Malaysia's legal framework is receptive to innovation in smart contracts, parties must observe both substantive and procedural contract requirements to minimise legal uncertainty and ensure enforceability.

Following Malaysia's example of legal adaptation, India does not have dedicated legislation for smart contracts; however, their legal enforceability is primarily determined by the Indian Contract Act, 1872 as the foundational statute governing all contractual relations in India.²⁴⁸ Under this Act, a smart contract, regardless of its form, will only be considered legally valid and enforceable if it satisfies the classic requirements of contract formation: (i) valid offer and acceptance,²⁴⁹ (ii) lawful consideration,²⁵⁰ (iii) intention to create legal relations,²⁵¹ and (iv) capacity of the parties to contract.²⁵² These basic requirements, codified in Sections 2, 10, and 11 of the Act, apply equally whether the agreement is made on paper or through automated blockchain code.²⁵³ In practice, the execution of smart contracts frequently involves actions such as clicking an 'I Agree' button or transferring digital assets, which can constitute valid offer and acceptance under Indian law.²⁵⁴

The Information Technology Act, 2000 further strengthens the legal status of smart contracts by explicitly recognizing the validity of

²⁴⁶ Shin Associates, "Enforceability of Smart Contracts in Malaysia," 2024.

²⁴⁷ Shin Associates.

²⁴⁸ India Code, "The Indian Contract Act," 1872.

²⁴⁹ India Code.

²⁵⁰ India Code.

²⁵¹ India Code.

²⁵² India Code.

²⁵³ India Code.

²⁵⁴ See also Satyansh Singh Parmar and Lavanyashree Raje Parmar, "Legal Examination of Smart Contracts Under Indian Law," *White Black Legal Law Journal* 2, no. 16 (2024): 4–6; India Code, "The Indian Contract Act."

electronic records, electronic contracts, and digital signatures. Section 10A of the Act guarantees the enforceability of contracts formed through electronic means, regardless of their electronic form. This provision is critical in establishing the legal effect of blockchain-based agreements, including smart contracts, as it removes the barrier of ‘form’ in digital contracting.²⁵⁵ In terms of evidence, the Indian Evidence Act, 1872, last amended in 2020, explicitly allows for the admissibility of electronic records in judicial proceedings under Section 65B. This provision states that information contained in an electronic record, including smart contracts and blockchain records, is admissible as evidence if its authenticity and integrity can be established in accordance with statutory requirements. As a result, parties can submit digital agreements to prove the existence, terms, and performance of a contract in court. Nevertheless, practical challenges remain regarding the verification and security of such electronic evidence.²⁵⁶

Academic and professional commentaries generally agree that Indian law, while technologically neutral, can flexibly accommodate the operation of smart contracts as long as substantive legal requirements are fulfilled.²⁵⁷ However, uncertainties persist, particularly regarding contracts involving cryptocurrencies due to their ambiguous legal status²⁵⁸ and technical risks such as coding errors or unintended automated execution, which may affect enforceability.²⁵⁹ Furthermore, compliance with statutory or regulatory requirements, including those relating to stamping, registration, or other formalities (for example, property transactions), may restrict the effectiveness or admissibility of certain smart contracts if such requirements are not met in digital form.²⁶⁰ In summary, the Indian legal system does not prohibit the use of smart contracts; rather, their enforceability depends on the satisfaction of both substantive and, where applicable, formal requirements prescribed under contract and information technology law.²⁶¹ Consequently, parties

²⁵⁵ India Code, “Information Technology Act,” 2000, Section 10A.

²⁵⁶ India Code, “Indian Evidence Act,” 1872, Section 65B.

²⁵⁷ Parmar and Parmar, “Legal Examination of Smart Contracts Under Indian Law.”

²⁵⁸ Parmar and Parmar.

²⁵⁹ Parmar and Parmar.

²⁶⁰ Parmar and Parmar.

²⁶¹ Parmar and Parmar.

deploying smart contracts in India must pay careful attention to these legal parameters to ensure their agreements are both valid and enforceable.²⁶²

While traditional contract principles provide an initial analytical framework, they do not resolve the jurisdictional and governance conflicts posed by decentralized smart contract execution. Smart contracts deployed on public blockchains may self-execute across borders, potentially bypassing mandatory consumer protection rules, regulatory intervention mechanisms, or public law safeguards embedded in domestic legal systems. This tension becomes acute where immutable execution conflicts with legal requirements for reversibility, suspension, or termination—such as emerging “kill switch” obligations and human-override mechanisms under EU digital regulation. In such contexts, smart contracts function less as autonomous legal instruments and more as hybrid technical arrangements whose enforceability remains contingent on overriding public law constraints and conflict-of-laws principles.

Extending the discussion from India’s rapidly evolving landscape, the regulation and enforceability of smart contracts in China are underpinned by a multi-layered legal framework that blends statutory innovation with doctrinal conservatism. The foundational statutory regime is the Law of the People’s Republic of China on Electronic Signature (adopted in 2004, effective in 2005, and most recently amended in 2015),²⁶³ which provides the primary basis for recognizing electronic agreements, including those executed on blockchain platforms. Under Article 3 of this law, the legal effect of a document shall not be denied solely on the grounds that the parties have agreed to use an electronic signature or data message, thereby granting electronic contracts formal equivalence with traditional paper-based agreements.²⁶⁴ However, the law delineates clear exceptions for certain legal relationships, such as marriage, adoption, succession, and the transfer of

²⁶² Parmar and Parmar.

²⁶³ Chinese Academy of Social Sciences, “Law of the People’s Republic of China on Electronic Signature,” 2024.

²⁶⁴ Chinese Academy of Social Sciences.

real estate rights, where electronic contracting is expressly excluded.²⁶⁵ Article 14 further strengthens the legal foundation for smart contracts by stipulating that a reliable electronic signature possesses equal legal force to a handwritten signature or seal, provided it meets the requirements of exclusivity, control, and detectability of alteration as detailed in Article 13.²⁶⁶ Complementary provisions, such as Articles 4 to 8, affirm that electronic data messages, including blockchain records, are legally equivalent to written documents if they can reliably represent their contents and are accessible for reference, and that such records cannot be rejected as evidence merely due to their digital form.²⁶⁷

Within this legal context, Chinese academic literature, such as the review by Wen and Fang, shows a broad consensus that smart contracts may, in principle, be treated as valid legal acts under Chinese contract law, provided they manifest the genuine intention of the parties and fulfill the substantive requirements of contract formation.²⁶⁸ These requirements encompass not only a clear expression of intent and lawful purpose but also compliance with any relevant formalities mandated by the Civil Code or other applicable statutes.²⁶⁹ Significantly, many Chinese scholars frame smart contracts as a modern evolution of electronic data interchange (EDI), thereby benefitting from the same statutory recognition accorded to electronic signatures and electronic records, an interpretation which provides strong doctrinal support for their enforceability in digital environments.²⁷⁰ While Chinese courts have increasingly begun to recognize the enforceability of digital and smart contracts, particularly where the parties' intention and technical reliability can be established. The academic debate is far from settled.²⁷¹ A number of commentators remain cautious, questioning whether smart

²⁶⁵ Chinese Academy of Social Sciences, Article 3 (exceptions: marriage, adoption, succession, transfer of real estate certain utilities, etc).

²⁶⁶ Chinese Academy of Social Sciences.

²⁶⁷ Chinese Academy of Social Sciences.

²⁶⁸ Qingmei Wen and Haowei Fang, "A Theoretical Review of Studying on Smart Contract in Blockchain Technology Revolution," *Ad Astra, Ahead of Print*, 2023, 5, <https://doi.org/10.53261/adastra20230702>.

²⁶⁹ Wen and Fang, "A Theoretical Review of Studying on Smart Contract in Blockchain Technology Revolution."

²⁷⁰ Wen and Fang.

²⁷¹ Wen and Fang.

contracts constituted solely as self-executing code, and absent any supporting traditional written agreement, truly satisfy the classical requirements of consensus and intent.²⁷² In such cases, courts may be compelled to conduct a multi-factor analysis, scrutinizing both the technical parameters of the smart contract and the surrounding circumstances to determine whether a legally binding agreement was in fact formed.²⁷³

Despite this generally enabling environment, China's regulatory approach remains conservative and principled, particularly in areas such as NFT royalties, fully automated cross-border contracts, and contracts involving significant anonymity or immutability.²⁷⁴ The principle articulated in the Civil Code, especially Article 153 concerning public order and good morals, serves as an important limitation: smart contracts that undermine transaction security, violate regulatory policy, or offend public order may be deemed invalid.²⁷⁵ Regulatory authorities, including the Supreme People's Court, have issued Opinions on Strengthening the Judicial Application of Blockchain (2022), which encourage the use of blockchain and smart contracts to improve efficiency, automate mediation and enforcement, and build a standardized judicial ecosystem.²⁷⁶ Empirical data demonstrates that while the adoption of smart contract technology in China is growing, its primary use remains in standardized, low-value digital transactions, product design, and automated business processes.²⁷⁷ Form 1 smart contracts, natural language contracts with automated performance, are routinely recognized, whereas hybrid (Form 2) and code-only (Form 3) smart contracts face legal ambiguity regarding their enforceability.²⁷⁸

In sum, China's legal and regulatory framework establishes that smart contracts, when executed in compliance with statutory

²⁷² Wen and Fang.

²⁷³ Wen and Fang.

²⁷⁴ Wen and Fang.

²⁷⁵ Wen and Fang.

²⁷⁶ Andrew Godwin, "Chinese Contract Law and Smart Contracts 中国合同法与智能合约 English-Chinese Definition," China Lexicon, 2025.

²⁷⁷ Wen and Fang, "A Theoretical Review of Studying on Smart Contract in Blockchain Technology Revolution."

²⁷⁸ Wen and Fang.

requirements including the use of reliable electronic signatures and clear intention, are generally enforceable. However, practical and doctrinal uncertainties remain, particularly for novel forms of smart contract that test the boundaries of traditional contract law and statutory regulation.²⁷⁹ In this respect, China's approach illustrates both the adaptability and the limits of technological innovation within a civil law tradition.

These differing frameworks mean that, although the legal groundwork for smart contracts is now well established in parts of Asia, enforcement, especially across jurisdictions and in areas such as automated royalty payments, remains contingent on marketplace practices and the evolving interpretation of national statutes.

Recent developments in NFT art exemplified by the generative AI-based practice of Emi Kusano reveal how smart contracts can transform not only provenance and proof of ownership but also the mechanisms for royalty allocation, collaborative value sharing, and global art market participation.²⁸⁰ Kusano, a multidisciplinary Tokyo-based artist, creates NFT artworks by merging AI-generated imagery with retro-futuristic cultural themes, often remixing elements from 1980s and 1990s Japanese pop culture. She mints these digital works as NFTs on blockchain platforms, encoding not only proof of authorship and originality but also programmable royalty logic that automatically splits proceeds with coders, AI model owners, and other creative collaborators. Her acclaimed "Zombie Zoo" project, developed during the COVID-19 lockdown with her young son, involved generating unique digital characters through a combination of AI and human input, then distributing them globally as NFTs. This hands-on use of generative AI and programmable smart contracts enables Kusano and other artists outside traditional art centers to achieve international reach, secure ongoing compensation from secondary sales, and transparently manage value distribution among all contributors via blockchain protocols.²⁸¹

However, Kusano's experience also highlights that, while smart contracts promise automated revenue distribution and creative

²⁷⁹ Wen and Fang.

²⁸⁰ WIPO, "Repainting the Past in a New Light with Generative Art," IP Advantage, 2025.

²⁸¹ WIPO.

collaboration, their effectiveness in protecting artists still depends on broader issues such as platform recognition, marketplace practices, and the development of legal standards issues that remain unresolved in the NFT and AI art space. She voices particular concern about the intersection of generative AI and intellectual property: “Artists like me remix different things to create an output that is entirely different from the input... Rather than the input, I believe the output matters, and if that output is something completely new and that’s never been seen, that should be considered as a form of art.” Kusano acknowledges that, although some mediums such as photography may be less vulnerable, illustrators, musicians, and actors face higher risks of unauthorized duplication and identity misuse by AI.²⁸²

Kusano’s perspective suggests that, even as smart contracts automate many transactional and distributive functions, substantive legal protections for creators are not guaranteed by code alone.²⁸³ The broader success of NFT and AI-driven art thus depends as much on the evolution of interoperable legal standards, responsible platform policies, and recognition of creative labor as on technical innovation itself. Kusano’s career, recognized by WIPO, ultimately illustrates both the empowering potential and persistent vulnerabilities of artists navigating copyright, compensation, and authorship in the digital era.²⁸⁴

Theoretical frameworks developed by scholars such as Lessig warn that the increasing regulatory power of code and platform standards risks consolidating control in the hands of technical and commercial gatekeepers, raising new questions of accountability and equity.²⁸⁵ Industry analysts further highlight that programmable NFTs offer significant efficiency and automation benefits for creators and platforms, enabling new revenue models and enhanced digital asset interactivity.²⁸⁶

²⁸² WIPO.

²⁸³ Indah Sri Utari et al., “Legal Protection for Child Sexual Violence Victims: Victimology Perspectives, Challenges, and Policy Solutions in Asia,” *Jurnal Suara Hukum* 8, no. 1 (2026): 40–77, <https://journal.unesa.ac.id/index.php/suarahukum/article/view/48307>.

²⁸⁴ WIPO, “Repainting the Past in a New Light with Generative Art.”

²⁸⁵ Lessig, *Code and Other Laws of Cyberspace*.

²⁸⁶ Jesse Anglen, “Exploring Programmable NFTs: Dynamic Benefits & Revolutionary Use Cases,” 2024.

However, as the OECD emphasizes, self-regulation and purely market-driven approaches have several limitations, “notably because [they] may lack transparency and fail to properly reflect the preferences of economic agents.” In the absence of a common regulatory framework, “competition issues may arise,” and dominant businesses may exploit self-regulation to develop “barriers to entry,” making it harder for new or marginalized creators to participate fairly.²⁸⁷ The OECD thus concludes that the success of self-regulatory and market-driven approaches “critically hinges on the capacity of governments to closely monitor practices and to engage in regular reviews of technical standards and codes of practice in an open and inclusive way, to avoid inappropriate market distortions.”²⁸⁸ Without this proactive governmental oversight and inclusive review process, there is a persistent risk that self-regulation may fail to reflect the broader interests of all stakeholders or may even entrench barriers to entry and competition. These tensions underscore that technological innovation alone cannot guarantee fair or inclusive outcomes and that the evolution of digital creative economies must be accompanied by adaptive legal frameworks and vigilant policy oversight.

In sum, the programmable rights revolution in NFTs and AI-generated art exemplifies the paradox of digital legal innovation: technical solutions promise frictionless enforcement but remain limited by deep legal and structural constraints. Without harmonized frameworks and inclusive governance, the digital art economy remains suspended between the ideal of code-driven justice and enduring legal inequities. Addressing these challenges requires regulatory harmonization, enforceable standards, and accessible dispute resolution to secure creators’ rights across platforms and borders.

Conclusion

This research set out to examine how current legal frameworks address the challenges posed by AI-generated and hybrid NFT artworks, with a particular focus on copyright attribution, the enforceability of

²⁸⁷ OECD/KDI, *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses*.

²⁸⁸ OECD/KDI.

smart contracts, and the recognition of blockchain-based evidence in cross-border contexts. The findings demonstrate that while certain jurisdictions such as the United States, the European Union, and several Asian countries have attempted to apply existing intellectual property principles to hybrid authorship, these approaches remain inconsistent and incomplete. The United States enforces a strict requirement for human authorship, the European Union adopts the standard of the author's own intellectual creation but applies it with variation between member states, and Asian jurisdictions such as China and Japan recognise certain AI-assisted works only when there is clear and substantial human input. The absence of a unified standard means that works created through human-machine collaboration are subject to legal uncertainty, often leaving creators with limited remedies and forcing reliance on private contractual arrangements or platform-specific rules.

The comparative analysis confirms that this fragmentation has significant practical consequences for creators and market participants. Divergent legal standards invite regulatory arbitrage, where parties choose jurisdictions most favourable to their position, and complicate the enforcement of rights in transnational digital art markets. Smaller or independent creators, particularly those from jurisdictions with underdeveloped intellectual property enforcement, face disproportionate risks of misappropriation and undervaluation of their work. This undermines the inclusive and decentralised vision often associated with blockchain-based art markets.

The possible application of these findings extends to both legislative reform and industry practice. Legislators should work toward harmonised rules on originality and attribution that recognise the reality of hybrid authorship without eroding the protection of human creativity. Such harmonisation could take the form of model provisions agreed at the international level, providing guidance for national laws and reducing uncertainty for cross-border transactions. The development of technical standards for blockchain provenance, including the admissibility of on-chain records as legal evidence, would further strengthen the enforceability of rights. At the industry level, NFT marketplaces could adopt transparent and enforceable policies aligned with international copyright norms, supported by smart contract

mechanisms that guarantee royalty payments to creators regardless of resale location.

Calls for comprehensive global harmonization through model laws or centralized drafting bodies risk overlooking the structural incentives that drive regulatory arbitrage and forum shopping in digital creative markets. Jurisdictional divergence is not merely a coordination failure but often reflects deliberate policy choices concerning innovation, enforcement capacity, and economic strategy. As long as these incentives persist, creators, platforms, and intermediaries will continue to route activity toward more permissive or predictable regimes. Law reform must therefore operate within, rather than against, a fragmented transnational legal landscape.

More fundamentally, the limits of global harmonization reflect enduring philosophical divisions within copyright law itself. Author-centric regimes, most prominently associated with the European tradition, protect personal expression and moral rights, treating authorship as an extension of human personality. Economically oriented systems, such as those of the United States and the United Kingdom, conceptualize copyright primarily as an instrument for incentive alignment and market efficiency. Technical standard-setting alone cannot reconcile the distinct normative commitments embodied by these approaches. Any credible law reform agenda must therefore acknowledge this irreducible divide rather than assume substantive convergence.

Rather than pursuing substantive harmonization of authorship or originality standards, law reform efforts should prioritize functional interoperability across jurisdictions. This includes shared disclosure obligations regarding AI involvement, baseline provenance documentation for AI-assisted works, and minimum safeguards against misattribution and data misuse. Such measures can reduce uncertainty and opportunistic forum shopping while preserving the normative autonomy of national copyright systems.

Therefore, the successful integration of AI and blockchain into the creative economy requires more than incremental adjustments to existing law. It demands a coordinated effort to design a new legal architecture that is capable of recognising complex authorship models, supporting technological solutions for rights management, and providing

predictable enforcement in the global digital marketplace. Without such an approach, the creative potential of AI-assisted works will remain constrained by fragmented regulation and market uncertainty, limiting the benefits for creators, consumers, and the cultural economy as a whole.

References

- Adhari, Ade, Fransisca Iriani Roesmala Dewi, Anis Widyawati, Darius Andana Haris, and Dwiky Chandra. 2025. "Rehabilitation through Reading: Evaluating Prisoners' Right to Literacy As a Tool to Reduce Recidivism". *Indonesian Journal of Criminal Law Studies* 10 (2): 659-84. <https://doi.org/10.15294/ijcls.v10i2.29687>.
- AI Verify Foundation. "What Is AI Verify – AI Verify Foundation," 2025.
- AI Verify Foundation Infocomm Media Development Authority (IMDA). "Model AI Governance Framework for Generative AI," 2024.
- AI21 Labs. "Private AI vs. Public AI: What Is the Difference?" AI21, 2025.
- Albagli, David, Toshio Dokei, Arthur M. Mitchell, and Shinsuke Yakura. "AI Watch: Global Regulatory Tracker - Japan," 2025.
- Anders, Lance, and Shrug. "ERC-4907: Rental NFT, an Extension of EIP-721," 2022.
- Anglen, Jesse. "Exploring Programmable NFTs: Dynamic Benefits & Revolutionary Use Cases," 2024.
- Annavi, Sam K. "AI Meets NFT: Fusion Fuels a New Era in Digital Art." *BlockchainTechs.Io*, 2025.
- ASEAN. "ASEAN Guide on AI Governance and Ethics Contents," 2024.
- Attorney-General's Chambers of Singapore. "Financial Services and Markets Act 2022 (No. 18 of 2022)," 2022.

- AWAPoint. "China's First AI-Generated Picture Copyright Infringement Case: Legal Implications," 2024.
- Beijing Internet Court. "Top Ten Typical Cases in Five Categories," 2023.
- Bertazzolo, Giacomo. "NFTs in the Digital Age: Cybersecurity Risks and AI-Powered Smart Contract Solution," 2023.
- Berto, Rebecca. "Blockchain Records: Is the Evidence Admissible? A Challenge for European Member States." *Civil Procedure Review* 10, no. 3 (2019).
- Blockchain Today. "AI-Generated NFTs and Their Impact on the Digital Art Market." Medium, 2025.
- BlockchainTechs.io. "How AI Generated NFT Art Is Shaping the Future of NFT Art Collections," 2025.
- Bommarito, Michael J, Jillian Bommarito, and Daniel Martin Katz. "The KL3M Data Project: Copyright-Clean Training Resources for Large Language Models," 2025.
- Borges, Natália Tavares, and Rui Pedro Rodrigues Leite. "Revolutionizing Contracts: The Impact of Blockchain Technology and Smart Contracts." *JustGov Research Paper No 2024-23*, 2024. <https://doi.org/10.2139/ssrn.5064863>.
- Calvo, Patrici. "Cryptoart: Ethical Challenges of the NFT Revolution." *Humanities and Social Sciences Communications* 11, no. 1 (2024): 370. <https://doi.org/10.1057/s41599-024-02872-2>.
- Chainalysis Team. "NFT Transaction Activity Stabilizing in 2022 After Explosive Growth in 2021." Chainalysis, 2022.
- Chinese Academy of Social Sciences. "Law of the People's Republic of China on Electronic Signature," 2024.
- Consensys Diligence. "Smart Contract Audits," 2025.
- Copyright.gov. Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence (2023).
- Dang, Fei. "Beijing Court Sentences Four People for Infringing Copyright by Using AI," 2025.

- Dyquiangco, Excel V. “Japan High Court Upholds Rejection of AI as Inventor in Patent Case.” Asia IP, 2025.
- Ekshian, Emily. “How NFT Royalties Work - and Sometimes Don’t.” Crypto Council for Innovation, 2023.
- Electronic Commerce Act. “Laws of Malaysia,” 2006.
- European Commission. “Blockchain and Web3 Strategy.” Shaping Europe’s Digital Future, 2025.
- . “European Blockchain Sandbox Best Practices Report, 2nd Cohort,” 2024.
- European Union Intellectual Property Office (EUIPO). *The Development of Generative Artificial Intelligence from a Copyright Perspective*. European Union Intellectual Property Office, 2025. <https://doi.org/10.2814/3893780>.
- European Union law. “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,” 2021.
- . “Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Artificial Intelligence (Artificial Intelligence Act) (2024).,” 2024.
- Eva-Maria Painer v Standard VerlagsGmbH and Others (Third Chamber). “Judgment of 1. 12. 2011 — Case C-145/10 Judgment of the Court (Third Chamber) 1 December 2011,” 2011.
- Federal Rules of Evidence. “Rule 901: Authenticating or Identifying Evidence,” 2025.
- Feist Publications Inc. “Rural Tel. Serv. Co.,” 1991.
- Filipi, Primavera De, and Aaron Wright. *Blockchain and the Law: The Rule of Code*. Harvard University Press, 2018.
- Financial Crimes Enforcement Network (FinCEN). “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies (FIN-2019-G001),” 2019.

- Gate.com. "Zora: Redefining Value in Digital Art," 2024.
- Ginsburg, Jane C. "Fifty Years of U.S. Copyright: Toward a Law of Authors' Rights?," 2022.
- Godwin, Andrew. "Chinese Contract Law and Smart Contracts 中国合同法与智能合约 English-Chinese Definition." China Lexicon, 2025.
- Grinbergs, Kristaps. "Implementing the ERC-2981 NFT Royalty Standard with Solidity - a Game-Changer for Creators to Receive Income from Every Sale." DEV Community, 2023.
- Guadamuz, Andres. "The Treachery of Images: Non-Fungible Tokens and Copyright." *Journal of Intellectual Property Law & Practice* 16, no. 12 (December 2021): 1367–85. <https://doi.org/10.1093/jiplp/jpab152>.
- Hagi, Andrei, and Julian Wright. "Artificial Intelligence and Competition Policy." *International Journal of Industrial Organization*, 2025, 103134. <https://doi.org/10.1016/j.ijindorg.2025.103134>.
- Health Products Act. "Singapore Statutes Online 2007," 2020.
- Health Sciences Authority (HSA). "Integrated Health Information Systems (IHIS) Ministry of Health (MOH), Artificial Intelligence in Healthcare Guidelines (AIHGle)," 2021.
- Iaia, Vincenzo. "The Elephant in the Room of EU Copyright Originality: Time to Unpack and Harmonize the Essential Requirement of Copyright." *The Journal of World Intellectual Property* 28, no. 2 (July 2025): 471–90. <https://doi.org/10.1111/jwip.12343>.
- Inc Artema Labs. "Systems and Methods for Facilitating Access to Token Content, Patent US20230385815A1, Issued May 24, 2023," 2023.
- India Code. "Indian Evidence Act," 1872.
- . "Information Technology Act," 2000.

- . “The Indian Contract Act,” 1872.
- Infocomm Media Development Authority (IMDA). “Singapore Launches Project Moonshot.” IMDA, 2024.
- Infocomm Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC). “Model Artificial Intelligence Governance Framework (Second Edition),” 2020.
- Infopaq International A/S v Danske Dagblades Forening. “Judgment of 16. 7. 2009 — Case c-5/08: Judgment of the Court (Fourth Chamber) 16 July 2009,” 2009.
- Internal Revenue Service. *IRS Notice 2014-21: Guidance on Virtual Currency*, 2014.
- Japan Copyright Office. “General Understanding on AI and Copyright in Japan,” 2024.
- Japanese Law Translation. “Outline of the Act on Promotion of Research and Development, and Utilization of AI-Related Technology (AI Act),” 2025.
- Jasperse, Joseph. “50-State Review of Cryptocurrency and Blockchain Regulation,” 2023.
- Kin, Lim Chong, and Cheryl Seah. “Artificial Intelligence 2025 - Singapore | Global Practice Guides | Chambers and Partners,” 2025.
- Kumtepe, Cemre Ç Kadioglu. *Defining Boundaries of Due Process in Blockchain Arbitration*. Radboud University Press, 2025. https://doi.org/10.54195/FMVV7173_CH02.
- Lai, Stanley, David Lim, Linda Shi, and Justin Tay. “Legal Implications – Beijing Internet Court Grants Copyright Protection to AI-Generated Artwork,” 2024.
- Langlais, Pierre-Carl, Carlos Rosas Hinostroza, Mattia Nee, Catherine Arnett, Pavel Chizhov, Eliot Krzystof Jones, Irène Girard, David Mach, Anastasia Stasenko, and Ivan P Yamshchikov. “Common Corpus: The Largest Collection of Ethical Data for LLM Pre-Training.” *ArXiv Preprint ArXiv:2506.01732*, 2025.

- Legal Information Institute. "17 U.S. Code § 107 - Limitations on Exclusive Rights: Fair Use," 1990.
- Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.
- Levola Hengelo BV v. Smilde Foods BV. "Case C-310/17," 2018.
- Lima, Eleonora. "AI Art and Public Literacy: The Miseducation of Ai-Da the Robot." *AI and Ethics* 4, no. 3 (2024): 841–54. <https://doi.org/10.1007/s43681-024-00488-5>.
- Linghan, Zhang, Yang Jianjun, Cheng Ying, Zhao Jingwu, Han Xuzhi, Zheng Zhifeng, and Xu Xiaoben. "Artificial Intelligence Law of the People's Republic of China (Draft for Suggestions from Scholars)." *Center for Security and Emerging Technology*. Accessed: Aug 16 (2024).
- Liu, Shuaiqi, and Qingxiao Zheng. "A Study of a Blockchain-Based Judicial Evidence Preservation Scheme." *Blockchain: Research and Applications* 5, no. 2 (2024): 100192. <https://doi.org/10.1016/j.bcra.2024.100192>.
- Lotti, Laura, Nick Houde, and Tara Merk. "Social Security for Web3 Work: A Preliminary Specification of the Design and Deployment of Solidarity Primitives for DAO Contributors." *SSRN Electronic Journal*, no. July (2023). <https://doi.org/10.2139/ssrn.4596552>.
- Lu, Tian. "The Implementation of Blockchain Technologies in Chinese Courts." *Stanford Journal of Blockchain Law & Policy* 4 (2021).
- Martin, Felix. "Why 'America First' Could End the Age of Arbitrage." Reuters, 2025.
- Masyhar, Ali, Indah Sri Utari, Usman, and Ahmad Zaharuddin Sani Ahmad Sabri. "Legal Challenges of Combating International Cyberterrorism: The NCB Interpol Indonesia and Global Cooperation." *Legality: Jurnal Ilmiah Hukum* 31, no. 2 (2023). <https://doi.org/10.22219/ljih.v31i2.29668>.
- Ministry of Foreign Affairs of Japan. "Hiroshima Process International

- Code of Conduct for Organizations Developing Advanced AI Systems,” 2024.
- Ministry of Internal Affairs and Communications. “Japan Conference Toward AI Network Society, AI Guidelines for Business – Version 1.0,” 2021.
- . “Japan Conference Toward AI Network Society, Interim Report on the Vision for Future Society Transformed by AI,” 2019.
- Monetary Authority of Singapore. “FinTech Regulatory Sandbox Guidelines,” 2022.
- . “Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore’s Financial Sector,” 2019.
- N.Y. Office of Information Technology Services. “Electronic Signatures and Records,” 2023.
- N.Y. State Technology Law. “N.Y. State Technology Law -Art. III,” 2016.
- National Science and Technology Development Agency (NSTDA), and Office of the National Digital Economy and Society Commission (ONDE). “Thailand National AI Strategy and Action Plan (2022–2027),” 2022.
- Nemeroff, Benjamin. “Understanding Decentralized Autonomous Organizations I Nym.” Nym, 2025.
- NFTGO. “NFT Annual Report 2024,” 2024.
- OECD/KDI. *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses*. Paris: OECD Publishing, 2021. <https://doi.org/10.1787/8fa190b5-en>.
- Official Journal of the European. “Regulation (EU) 2024/1689 on Harmonised Rules on Artificial Intelligence (AI Act), Pub. L. 2024/1689, Union,” 2024.
- OpenSea Help Center. “OpenSea Help Center,” 2024.
- Organisation for Economic Co-operation and Development (OECD).

- “The Digital Transformation of SMEs,” 2021.
- Parmar, Satyansh Singh, and Lavanyashree Raje Parmar. “Legal Examination of Smart Contracts Under Indian Law.” *White Black Legal Law Journal* 2, no. 16 (2024): 4–6.
- Perlmutter, Thaler v. “United States District Court for the District of Columbia: Memorandum Opinion,” 2023.
- Qadir, S., and G. Parker. “NFT Royalties: The \$1.8bn Question.” *Galaxy*, 2022.
- Ramirez Lopez, Leonardo J, and Genesis G Morillo Ledezma. “Employing Blockchain, NFTs, and Digital Certificates for Unparalleled Authenticity and Data Protection in Source Code: A Systematic Review.” *Computers*, 2025. <https://doi.org/10.3390/computers14040131>.
- Regulation EU. “Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA),” 2023.
- . “Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data (Data Act),” 2023.
- . “Regulation (EU) 910/2014 as Amended by Regulation (EU) 2024/1183 on Establishing the European Digital Identity Framework,” 2024.
- . “Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (EIDAS Regulation),” 2014.
- Road Traffic Act 1961. “Singapore Statutes Online,” 2020.
- Rose, Mark. *Authors and Owners: The Invention of Copyright*. Cambridge, MA: Harvard University Press, 1993. <https://doi.org/10.2307/3117041>.
- Ruiqiang, Li, Brian Yecies, Qin Wang, Shiping Chen, and Jun Shen. “Empowering Visual Artists with Tokenized Digital Assets with NFTs,” 2024.

- Sautoy, Marcus du. *The Creativity Code: How AI Is Learning to Write, Paint and Thinkd*. London: Fourth Estate, 2019.
- Sheposh, Richard. "Garbage in, Garbage out (GIGO)." EBSCO Research Starters: Computer Science, 2024.
- Shin Associates. "Enforceability of Smart Contracts in Malaysia," 2024.
- Singapore Legal Advice. "Using Smart Contracts in Singapore: Benefits and Risks," 2024.
- Singapore Statutes Online. "Electronic Transactions Act 2010," 2010.
- Singh, Gurinder, Vikas Garg, and Pooja Tiwari. *Introduction to Blockchain Technology. Transforming Cybersecurity Solutions Using Blockchain*. Springer, 2021.
https://doi.org/10.1007/978-981-33-6858-3_1.
- Singh, Sudhanshu. "Vietnam Passes First-Ever Law on Digital Technology Industry," 2025.
- Smart Nation and Digital Government Office. *Singapore National AI Strategy 2.0*, 2023.
- Soh, Jerrold, Josh Kok Tong Lee, and Felix Tan. "State of Legal Innovation in the Asia Pacific," 2019.
- Splits Help Center. "Using Manifold with Splits." Splits, 2024.
- Sun, Yao, Ann Majchrzak, and Arvind Malhotra. "593Open Innovation Theories." Edited by Henry Chesbrough, Agnieszka Radziwon, Wim Vanhaverbeke, and Joel West. *The Oxford Handbook of Open Innovation*. Oxford University Press, February 2024.
<https://doi.org/10.1093/oxfordhb/9780192899798.013.35>.
- Susnjara, Stephanie, and Ian Smalley. "What Is Blockchain?," 2025.
- Terekhova, Anastasiia. "The Impact of AI-Generated NFT Art on the Global Art Market: Trends and Perspectives." *Scientific Journal of Bielsko-Biala School of Finance and Law* 29, no. 1 SE-Articles (March 2025). <https://doi.org/10.19192/wsfiip.sj1.2025.8>.
- Tiku, Nitasha. "New Research Shows It's Possible to Build Powerful AI without Violating Copyright - The Washington Post," 2025.

- U.S. Commodity Futures Trading Commission. "CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets," 2018.
- U.S. Copyright Office. *Compendium of U.S. Copyright Office Practices*, Third Edition, §§ 802.5(C), 808.7(C) (2021).
- U.S. Government Printing Office. "Electronic Signatures in Global and National Commerce Act, Pub. L. Public Law 106–229, 15 U.S.C. § 7001 et Seq," 2000.
- U.S. Securities and Exchange Commission. "Framework for 'Investment Contract' Analysis of Digital Assets," 2019.
- Uniform Laws. "Uniform Electronic Transactions Act, Pub. L. ULC 1999," 1999.
- United Nations Commission on International Trade Law. "UNCITRAL Model Law on Electronic Commerce (1996) with Additional Article 5 Bis as Adopted in 1998," 1996.
- Utari, Indah Sri, Ubaidillah Kamal, Diandra Preludio Ramada, Benny Sumardiana, and Bhanu Prakash Nunna. "Legal Protection for Child Sexual Violence Victims: Victimology Perspectives, Challenges, and Policy Solutions in Asia." *Jurnal Suara Hukum* 8, no. 1 (2026): 40–77. <https://journal.unesa.ac.id/index.php/suarahukum/article/view/48307>.
- Utari, Indah Sri, Diandra Preludio Ramada, Ubaidillah Kamal, Ratih Damayanti, and Nizamuddin Alias. "The Digital Sanctuary: Forging Legal And Ethical Frameworks For Interfaith Coexistence Online." *Contemporary Issues on Interfaith Law and Society* 4, no. 2 (2025). <https://doi.org/10.15294/ciils.v4i2.35309>.
- WAC Lab. "Are 95% Of NFTs Really Worthless? Let's Take A Closer Look At The Market." Web3 for the Arts and Culture, 2023.
- Wang, Xukang, Ying Cheng Wu, and Zhe Ma. "Blockchain in the Courtroom: Exploring Its Evidentiary Significance and

- Procedural Implications in U.S. Judicial Processes.” *Frontiers in Blockchain* 7 (2024).
<https://doi.org/10.3389/fbloc.2024.1306058>.
- Wen, Qingmei, and Haowei Fang. “A Theoretical Review of Studying on Smart Contract in Blockchain Technology Revolution.” *Ad Astra, Ahead of Print*, 2023.
<https://doi.org/10.53261/adastra20230702>.
- Widyawati, Anis, Ade Adhari, Ali Masyhar, Bearly Deo Syahputra, and Didik Purnomo. “Dynamics of the Penitentiary System, Transparent and Accountable Handling of Criminal Cases in Criminal Execution Law in Southeast Asia: Convergence and Divergence of International Perspectives.” *Indonesia Law Review* 15, no. 1 (2025): 15–35.
<https://doi.org/10.15742/ilrev.v15n1.1>.
- WIPO. “Repainting the Past in a New Light with Generative Art.” IP Advantage, 2025.
- Woodmansee, Martha. “The Genius and the Copyright: Economic and Legal Conditions of the Emergence of the ‘Author.’” *Eighteenth-Century Studies* 17, no. 4 (August 1984): 425–48.
<https://doi.org/10.2307/2738129>.
- World Intellectual Property Organization. *Overview of the International Protection of Copyright and Related Rights: From the Berne Convention to the WIPO Copyright Treaty (WIPO/CR/DAM/05/8)*. Geneva: World Intellectual Property Organization, 2025.
- . Patent Landscape Report: Generative Artificial Intelligence. Geneva, issued 2024. <https://doi.org/10.34667/tind.49740>.
- . *WIPO Scoping Study on IP Enforcement in Digital Creative Markets*. Geneva, 2024.
- WPO. *Blockchain Technologies and IP Ecosystems: A WIPO White Paper*. Geneva, Switzerland: World Intellectual Property Organization, 2022.

- Yi Tenen, Dennis. "Author—Anonymous and Distributed." *New Techno-Humanities* 4, no. 1 (2024): 54–57. <https://doi.org/10.1016/j.techum.2024.07.001>.
- Zambrano, Raúl. "Taming the Beast: Harnessing Blockchains in Developing Country Governments." *Frontiers in Blockchain* Volume 2- (2020). <https://doi.org/10.3389/fbloc.2019.00027>.

Acknowledgment

The authors wish to express their sincere gratitude to their faculty members and cooperation partners for invaluable guidance, insightful feedback, and sustained encouragement throughout the development of this research. The authors also acknowledge the support of institutional peers whose comments and discussions contributed to the refinement of the analysis. Appreciation is extended to the anonymous reviewers for their constructive observations, which significantly improved the quality of this article. All remaining errors and interpretations remain the sole responsibility of the authors.

Funding Information

None.

Conflicting Interest Statement

There is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.