INTELLECTUAL PROPERTY RIGHTS AND THE DIGITAL ECONOMY: CHALLENGES OF ENFORCEMENT IN THE AGE OF ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN

Sudiksha Kumari, LL.M, IILM University.

ABSTRACT

The advent of Artificial Intelligence and Blockchain technologies has radically transformed the digital economy, offering new paradigms for content creation, distribution, and ownership. However, these advancements also pose significant challenges to the enforcement of Intellectual Property Rights. This paper critically examines the doctrinal foundations of IPR enforcement in the context of emerging technologies, while also presenting empirical data to assess the efficacy of current legal frameworks.

Doctrinally, the research explores traditional principles of copyright, patent, and trademark law, and interrogates their applicability in digital contexts driven by autonomous AI-generated content and decentralized blockchain infrastructures. Particular attention is given to issues such as authorship attribution in AI-generated works, the traceability of infringement in decentralized networks, and the jurisdictional complexities arising from transnational digital transactions. The analysis reveals a growing tension between established legal doctrines and the decentralized, borderless nature of digital innovation.

Empirically, the paper reviews enforcement trends through case law analysis, international treaty developments, and quantitative data on IP infringement reported across digital platforms. It also includes stakeholder interviews and surveys involving legal practitioners, tech developers, and IP owners, which highlight gaps in awareness, enforcement mechanisms, and regulatory harmonization.

This study concludes that while AI and blockchain technologies offer potential tools for IPR protection—such as smart contracts and automated rights management—they also necessitate urgent legal reform. It argues for a hybrid regulatory approach that blends technological solutions with doctrinal evolution, and proposes policy recommendations aimed at strengthening cross-border enforcement, legal certainty, and adaptive regulatory frameworks.

Keywords: WIPO, EU Copyrights, Trips, Digital Millennium Copyright, Intellectual property.

Introduction

The digital economy, which is marked by accelerating technologies, pervasive presence of the Internet, and widespread occurrence of digital content, has radically reshaped the production, dissemination, and protection of intellectual property (IP). Concurrently, new technologies like Artificial Intelligence (AI) and blockchain technology pose both novel opportunities and new challenges to the protection of intellectual property rights (IPRs). AI can create original works, reproduce styles, create inventions, or handle voluminous amounts of data, which makes old conceptions of authorship, originality, and infringement difficult. Blockchain, whose immutability, decentralization, transparency, and possibility of inserting ownership or transaction records, holds promising potential for IP registration, monitoring, licensing, and enforcement but also creates novel legal, technical, and jurisdictional challenges. In the 21st century, the digital economy has emerged as a dominant force, reshaping how individuals, businesses, and governments create, share, and monetize knowledge, data, and innovation. At the heart of this transformation lies intellectual property (IP)—the legal framework that protects intangible assets such as inventions, literary and artistic works, software, designs, and brand identities. While the digital economy has expanded opportunities for creators and innovators, it has also introduced profound challenges in the maintenance and enforcement of intellectual property rights (IPR). These challenges are driven by the borderless nature of the internet, rapid technological advances, and the proliferation of digital content. Traditionally, intellectual property was easier to control and protect because it was mostly physical—books, music CDs, patented machinery, etc. However, in the digital age, IP has become predominantly intangible and easily replicable. A single click can duplicate and distribute copyrighted music, films, software, or eBooks to millions of users across the globe, often without the original creator's knowledge or consent. (ieeexplore, 2025)

Moreover, the nature of creation itself has evolved. Innovations now often involve data analytics, artificial intelligence (AI), machine learning algorithms, and blockchain technology. These developments have raised new legal and ethical questions around authorship, ownership, and enforcement. For example, who owns content generated by AI systems? Does it fall under traditional copyright, or is a new category of IP law needed?

Digital goods can be copied and distributed instantly, often anonymously. This ease of duplication poses a significant threat to rights holders, especially in industries such as music,

publishing, and software development. Piracy remains widespread, despite improved legal enforcement and technological countermeasures. Websites offering illegal downloads or streams of copyrighted content often reappear under new domains after being shut down. IP laws are territorial in nature, meaning they are enforced at the national level. However, the internet is borderless, allowing IP infringement to occur across jurisdictions with little legal clarity or consistency. A copyrighted movie might be uploaded illegally in one country and accessed by users worldwide. While some international treaties such as TRIPS (Trade-Related Aspects of Intellectual Property Rights) and WIPO (World Intellectual Property Organization) attempt to harmonize laws, enforcement remains uneven and complex. Technologies like blockchain, AI, 3D printing, and NFTs have created new forms of content and value. However, IP regulations have not kept pace with these innovations. In the case of AI-generated art or code, the current legal frameworks often fail to define who holds the rights—whether it's the user, the developer of the AI, or the AI itself. Much of the digital content consumed today is hosted on platforms such as YouTube, TikTok, Facebook, and GitHub. These platforms must balance user freedom with IP compliance, leading to content takedowns, demonetization, and algorithmic filtering. However, the sheer volume of user-generated content makes manual enforcement nearly impossible, resulting in both under-enforcement and over-censorship. (ieeexplore, 2025)

This article analyzes the problem of enforcing IPRs in the digital economy in the dual forces of blockchain and AI. We discuss how current legal and institutional orders are under strain, and what is stated by literature regarding technological and legal advancements to solve the problems, and provide critical analysis, findings, and recommendations.

Research questions:

- What are the main enforcement issues to IP rights presented by blockchain and AI technologies?
- How effective are the current technical, legal, and policy tools at addressing these challenges?
- What models or reforms could more balance innovation, enforcement, and creators' rights in this new setting?

Literature Review

Literature on IP enforcement in the era of AI and blockchain draws from several fields: law, computer science, policy studies, and economics. Important themes that arise are:

Authorship, Inventorship, Originality: Numerous papers explore how the content created by AI belongs (or does not belong) within current doctrines of copyright or patent law. For example, some jurisdictions mandate a human being as the author. Central to it all is the idea of "human creativity."Training Data and Prior Art: AI systems are trained on large datasets, frequently copyrighted material. This causes problems of unauthorized use, fair use, prior art for patent novelty, and dataset transparency.

Detection and Monitoring: How to detect infringement in AI-generated outputs: finding similarity, handling derivative works, measuring infringement, and handling false positives/negatives. Papers such as CopyScope and CopyJudge suggest technical frameworks for measuring infringement. (arxiv, 2025)

Blockchain for IP Management: Several proposed models/frameworks employing blockchain for IP registration, timestamping, tracing transactions, smart contracts for licensing or royalty, and immutable ownership records are established through literature. Some such examples include B2IPTS, SecureRights, etc.

Legal Recognition, Jurisdiction, Interoperability: Most papers highlight that legal systems are still adjusting gradually blockchain-based records are not invariably accepted in courts, jurisdictional uncertainty in decentralised frameworks, variations across nations, data privacy and regulatory concerns.Ethical, political, economic aspects: Issues regarding incentive to innovate, business models, equity (who profits), risk of IP being exploited or abused (e.g. overblocking, chilling effects), transparency, biases.In total, the literature provides numerous analyses of the issues, a few technical and legal fixes, yet also points out that enforcement (in practice) continues to be challenging under existing laws & systems. (legalraonline, 2025)

Research Methodology

Since this is more or less a normative and analytic study and not empirical field research, the methodology employed is:

Doctrinal Legal Research: Scrutiny of statutes, case law, legal precedents in different jurisdictions (e.g. U.S., EU, India, U.K.) to know how authorship, inventorship, originality, enforcement, liability are addressed, particularly in AI scenarios.

Technical Literature Survey: Scrutiny of computer science and engineering literature on detection of infringement tools, IP protection frameworks (watermarking, fingerprinting, similarity detection, etc.) and blockchain-based IP systems.

Comparative Case Studies: Studying emblematic cases or recent controversies between AI and IP (e.g., litigation against AI companies, cases such as DABUS in UK concerning AI inventorship) and real-life blockchain-based IP implementation.

Critical Policy Analysis: Assessing legal, technical, and socio-economic implications; evaluating gaps, risks, and trade-offs. Limitations: Insufficiency of publicly available, high-quality data in most jurisdictions; numerous still-pending cases with no ultimate rulings; constantly changing technology so some literature is extremely recent and provisional.

Body: Challenges of Enforcement

The enforcement challenges are examined in detail under two broad headings (AI-related challenges, blockchain-related challenges), followed by cross-cutting concerns.

- AI-Related Challenges
- Authorship, Inventorship, Human Creativity

Most laws demand a human inventor or author. Autonomous or semi-autonomous AI entities create uncertainty: is the user, the designer of the tool, or the AI the author? Examples like DABUS demonstrate challenges to inventorship.

Standard of originality: AI content could be derivative or extremely evocative of the works that already exist; establishing whether they cross "originality" thresholds is difficult. In addition, copyright legislation in most jurisdictions does not acknowledge non-human authorship.

Training Data, Fair Use, and AI-Generated Prior Art

Large-scale ingestion of copyrighted works in training data leads to disputes. Are these uses

fair use (or similar doctrines elsewhere)? What about non-consensual or license-free uses?

AI-generated prior art: if AI's outputs are novel or relevant, but stored in proprietary or inaccessible systems, can they count as prior art in patent law? The issue of public accessibility arises.

Detection, Monitoring, and Proof

Difficulty in detection of infringement: AI-generated content can infringe in non-verbatim ways; similarity or derivative works require advanced algorithms. Also, very high false positive risk.

Attribution: it is legally and technically challenging to trace who is to be held accountable (user prompt-giver, AI model operator, model owner). Also, to trace back to training datasets.

ANI v. OpenAI (Delhi High Court, filed November 2024)

Facts: ANI (Asian News International) alleges that OpenAI used ANI's news content (copyrighted) to train its models without permission, and that ChatGPT sometimes reproduces content verbatim or "substantially similar" to ANI's works, as well as false attributions ("hallucinations"). ANI seeks damages and an injunction. (lawjournal, 2024)

Legal questions: whether consumption of copyrighted material for training (storage, reproduction) constitutes infringement under Indian law; whether "fair dealing" or other statutory exceptions can be invoked; whether the Indian courts have jurisdiction; impact of domestic vs foreign situs of servers.

Importance: This is likely the cleanest test case in India of AI-training versus copyright. It has the potential to set precedent about how Indian courts view LLMs and how much actionable training on copyrighted material there can be.

Scale, Speed, and Anonymity

AI facilitates mass creation of content, speedy transmission across borders. Enforcement agencies are often in no position for volume, cross-jurisdictional enforcement.

Operators can be anonymous or pseudonymous; takedown, enforcement, and liability become

complex.

- The Insurance Universe
- Blockchain-Related Challenges
- Legal Recognition of Blockchain Records & Smart Contracts

While blockchain can provide recording of ownership, timestamps, assignments, legal systems largely fail to fully accept blockchain entries or smart contracts as legally binding proof or enforceable contracts without further notarization (e.g. court acknowledgment).Smart contracts processing licensing or royalties are in question regarding enforceability under law, interpretation, resolution of disputes, and liability.

Jurisdiction, Decentralization, Interoperability

Blockchain networks are decentralized, cross-border. Jurisdictional concerns: what law governs? Which court can hear the matter? To what extent are judgments enforceable across borders?

There is frequently a lack of interoperability between disparate blockchain systems, or between blockchain systems and conventional registries. Data silos, in compatible standards hinder seamless coordination.

Case Law Example: Viacom International Inc. v. YouTube, Inc. (2010)-

Delhi High Court Aishwarya Rai Bachchan / Abhishek Bachchan personality / publicity rights and AI images (very recent)

Facts: The Delhi High Court ordered removal/takedown/banning of websites that used AI-generated images and names of Abhishek Bachchan (in connection with Aishwarya Rai's plea) without authorization, using their persona.

Legal questions: Protection of personality/publicity rights; abuse of identity by use of AI-created content; defamation, misrepresentation; remedy in the virtual world (takedowns, blocking).

Importance: Demonstrates the courts are considering AI-created images/persona-use as actual legal harm under Indian law, particularly under the tort/personal rights framework. This case doesn't yet include blockchain/NFT but is applicable for the AI abuse/personal identity aspect.

Facts:

Viacom (owner of MTV, Comedy Central, etc.) sued YouTube and its parent company Google for copyright infringement, claiming that YouTube hosted thousands of unauthorized video clips of Viacom content uploaded by users.

Viacom argued that:

- YouTube was aware of the infringing content.
- YouTube benefited financially from the content (through ads).
- YouTube did not act fast enough to remove infringing videos.

YouTube defended itself using the Digital Millennium Copyright Act (DMCA) safe harbor provision, which protects platforms as long as they remove infringing content when notified.

Ruling:

- In 2010, the district court ruled in favor of YouTube, stating that it complied with DMCA and did not have actual knowledge of specific infringements.
- The case was appealed and partially reversed, but in 2013, the parties settled out of court.

Significance:

- This case highlighted the complex balance between platform responsibility and user freedom.
- It reinforced the role of the DMCA safe harbor, showing that digital platforms are not automatically liable if they respond appropriately to takedown requests.
- It pushed platforms like YouTube to invest in better content recognition tools, like

Content ID, to proactively manage IP issues.

Strategies for Protecting IP in the Digital Economy

To address these challenges, various stakeholders—governments, private companies, creators, and consumers—are adopting multi-layered strategies to protect intellectual property in the digital space.

1. Technological Safeguards

- Digital Rights Management (DRM): Software tools that control how digital content is used, copied, or shared. DRM is common in eBooks, video streaming services, and software licensing.

- Content fingerprinting: Platforms like YouTube use AI-based tools (e.g., Content ID) to detect copyrighted material and take action automatically.

- Watermarking and encryption: These methods help identify the original source and reduce unauthorized distribution.

2. Legal and Policy Reforms

Governments are modernizing IPR laws to fit digital realities. For instance:

- The Digital Millennium Copyright Act (DMCA) in the United States provides a framework for takedown procedures on online platforms.

- The EU's Copyright Directive (2019) introduced stricter obligations for content-sharing platforms to prevent IP violations.

These policies aim to strike a balance between innovation, content sharing, and protection of rights.

3. International Cooperation

Given the cross-border nature of digital infringement, international cooperation is essential. Treaties like TRIPS and conventions under the WIPO encourage countries to adopt minimum standards of IP protection and enforcement. Regional bodies like the European Union are also

working on cross-border enforcement mechanisms. (ijalr.in, 2025)

4. Blockchain and NFTs

Blockchain technology offers decentralized and immutable records of ownership. This can be used to:

- Register IP rights on a distributed ledger.
- Track provenance and authenticity of digital assets.
- Issue Non-Fungible Tokens (NFTs) that act as proof of ownership for digital art, music, and other content.

Transparency vs Privacy, Data Protection

Blockchain's openness is at odds with confidentiality needed in some IP situations (unpublished works, trade secrets). Additionally, privacy legislation (such as GDPR) can impose restrictions on data that can be stored or revealed, Scalability, Cost, Technical Problems.

- Blockchain systems (particularly public ones) can have inherent maximums on transaction throughput, high transaction costs, energy use, etc. Concerns regarding whether they are scalable enough to accommodate high volume of IP transactions.
- Ensuring proper data entry: garbage-in, garbage-out. Malicious (or incorrect) ownership or assignment claims inputted, the system can retain errors.
    - LAB Blockchain Summit
    - Cross-Cutting Challenges
    - Legal and Regulatory

GapsStatutes and regulations were largely developed prior to AI and blockchain technology. They probably do not foresee such matters as non-human authorship, decentralized

recordkeeping, smart contract licensing. Legal frameworks fall behind. Literature reveals demands for adjustment.

Enforcement Capacity and Institutions

Courts, IP offices, enforcement authorities frequently neither have the technical knowledge, resources, nor procedures to address AI or blockchain related disputes. Smart contract disputes may not have guidelines in some jurisdictions, blockchain evidence, identifying AI-based infringement.

Economic Incentives vs Innovation

IP enforcement that is too restrictive can stop innovation, prevent positive uses of AI (for transformative works, research, training, remixing). It is essential to balance creators' rights with public interest, equity, innovation.

Also, enforcement cost is high for most creators (particularly small ones). Ethics, Bias, FairnessDetection processes may be biased in AI systems (e.g., overflag works by under-represented creators). Also, transparency (explainability) of AI decisions in enforcement is essential for due process. (ijalr.in, 2025)

Critical Analysis

Here, I analyse the pros and cons of existing measures and whether the solutions proposed solve the issues satisfactorily.

Strengths of Emerging Approaches

Technical Tools: Models like CopyScope, CopyJudge illustrate algorithmic solutions are more and more advanced, making quantification of similarity, detection of likely infringement, mitigation options. These are tangible tools for enforcement agencies and rights holders.

Blockchain registries and frameworks: Initiatives like SecureRights, B2IPTS, etc., illustrate proof-of-concepts for timestamping, immutable ownership records, licensing automation using smart contracts. These can decrease disputes on ownership and assist traceability.

Legal precedents & policy evolution: Certain cases (e.g. in copyright law, fair use doctrine, AI

cases) are stretching the boundaries. Also, regulatory agencies are looking at revisions, recognizing that existing laws require transformation. (omnuslaw, 2024)

Weaknesses, Gaps, Risks

Ambiguity persists: Even with tools, few legal systems have established clearly who owns works created by AI, or how to deal with non-human authorship. Legal uncertainty deters investment and can result in conflicting decisions.

Overdependence on technical detection: Technical detectors can make mistakes false positives, inability to perceive context (fair use, transformative uses), derivative vs original, style vs substance. Misuse has the potential to harm creators or stifle legitimate uses.

Blockchain overpromised?: Technically strong, but in practice, adoption is constrained. Legal acceptance, standardization, interoperability, cost, and privacy issues constrain broad enforceability. Also, blockchain is not the solution to all issues e.g., establishing that the entry represents true, legal ownership, or handling misregistration or illegitimate entries.Jurisdictional complexity: Cross-border enforcement remains a key stumbling block. Even with blockchain or AI detection evidence, enforcement needs courts, legal acceptance, cross-border coordination, which is expensive and time-consuming.

Incentives and power asymmetries: Big firms with resources control technological enforcement, detection tools, and can influence norms. Small creators are usually disadvantaged.

Privacy and ethical concerns: Leaky systems disclose data; detection algorithms reinforce biases; over-monitoring, censorship, or speech chilling risks are present.

Are Proposed Remedies Adequate?

Most suggested reforms are encouraging but incomplete. For instance, revamping statutes to enable intelligent definitions of authorship/inventorship, urging or requiring disclosure/licensing of training data, accepting blockchain records, facilitating standard smart contract templates these are helpful. But without harmonization, resource allocation, institutional capacity, numerous challenges lie ahead for real enforcement.

Findings and Suggestions-

Here are the findings and suggestions based on the literature and critical analysis.

Findings-

Substantial legal ambiguity regarding authorship, inventorship, ownership of AI-created works continues to exist, particularly when the role of humans is limited or not specified.Technical aids are on the rise but still short of comprehensive enforcement, particularly concerning identifying derivative works, contextual uses (fair use), or quantifying infringement accurately. Blockchain offers robust promise for record-keeping, transparency and tracing, but structural legal and regulatory acceptance, and standardization and interoperability, is behind. Cross-border and jurisdictional issues are significant hurdles enforcement across different regimes is complicated and expensive.Cost and capacity limitations on smaller creators, underfunded jurisdictions, or less advanced legal systems result in many not receiving the benefit of existing tools or legal recourse.Balance between innovation and protection is precarious overinclusive or overly mechanical enforcement chills useful purposes; but lax enforcement depletes the incentive to produce.

Suggestions-

To more effectively tackle enforcement issues, the following practices and reforms are proposed:

Legal Framework Reform

Clarify authorship/inventorship criteria in law: Establish criteria for human v AI contributions; potentially introduce intermediate models or co-authorship systems.

Modernize statutes to explicitly acknowledge blockchain records as admissible evidence of ownership, assignment, licensing. Moreover, legal principles regarding smart contracts, digital licensing, and royalty enforcement.

Clarify treatment of training data: Doctrinally establish what fair use (or equivalents) for AI models are; perhaps mandate disclosure or licensing of training data in some situations.

Harmonization across jurisdictions: International agreements or treaties can facilitate

standardization of acknowledgment of AI matters, blockchain proofs, cross-border enforcement.

Technical and Institutional Measures-

Invest in more effective detection tools: improved models for similarity, derivative works, explainability, minimizing false positives and false negatives.

Encourage standardization of blockchain IP registries: shared data formats, interoperable systems, permissioned or consortium blockchains where appropriate.

Capacity building for IP offices, judges, regulators: AI, blockchain, technical evidence, data science training.

Procedural & Evidentiary Innovations-

Design processes to enable faster adjudication in IP disputes relating to digital/AI content. For instance, special courts or IP arbitration panels.

Evidence handling: accept blockchain-based timestamped records, logs, smart contract transactions; create standards for validating technical evidence.

Foster transparency through mandatory audit trails of datasets, provenance, provenance of content creation by the owners of AI models.

Policy and Economic Measures-

Promote small creators: discounted legal assistance, lower registration mechanisms, affordable tools for infringement monitoring.

Incentives for licensing: marketplaces, platforms, providers of AI models should bargain on licensing regimes; collective licensing for mass consumption of copyrighted content, maybe. Guidelines for responsible use of AI, bias reduction, fairness in enforcement ensure that detection/enforcement isn't overly burdensome on some creators.

Public Awareness and Stakeholder Engagement-

Educate creators, users, platforms, policymakers regarding rights, risks, tools (blockchain,

detection, licensing).

Multi-stakeholder governance: engage creators, tech developers, legal scholars, policymakers in the crafting of frameworks, possibly in standards bodies.

Conclusion

The nexus of Artificial Intelligence, blockchain, and intellectual property rights in the digital economy offers both huge opportunities and significant challenges. While AI may create new work at scale, emulate or derive style, and accelerate innovation, it puts pressure on conventional legal notions of authorship, originality, and responsibility. Blockchain offers immutable history, transparent ownership, smart contracting, and possibly traceable enforcement, but its legal status, interoperability, and costs make it less effective currently.To effectively enforce IP rights in this era, a multi-faceted strategy must be followed. Legal reforms to clarify authorship/inventorship, new forms of evidence, harmonization among jurisdictions; technical advancements in detection and blockchain technologies; capacity building; and delicate balancing of rights versus innovation and public interest. In conclusion, the digital economy has both amplified the value of intellectual property and increased the difficulty of protecting it. The ease of copying, global distribution, and the rise of new technologies challenge traditional IP models. However, through a combination of technological tools, legal reforms, international cooperation, and innovative business models, it is possible to maintain and enforce intellectual property rights effectively in the digital age.As the digital economy continues to evolve, so too must the frameworks that protect the creativity and innovation that fuel it. The key will be balancing protection with access, ownership with openness, and enforcement with ethical responsibility.

If the reforms are carefully carried out, the digital economy can both enable strong innovation and equitable protection of creators' rights. Without them, there is potential for legal vacuums, suppression of creativity, and more infringing behavior.